Full

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 June 2002 (27.06.2002)

PCT

(10) International Publication Number
WO 02/51150 A2

(51) International Patent Classification[7]: H04N 7/167

(21) International Application Number: PCT/JP01/11104

(22) International Filing Date: 18 December 2001 (18.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2000-383345 18 December 2000 (18.12.2000) JP

(71) Applicant *(for all designated States except US)*: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. [JP/JP]; 1006, Oazakadoma, Kadoma-shi, Osaka 571-8501 (JP).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MATSUZAKI, Natsume [JP/JP]; 1-6-7-803, Aomadaninishi, Minou-shi, Osaka 562-0023 (JP). TATEBAYASHI, Makoto [JP/JP]; 1-16-21, Mefu, Takarazuka-shi, Hyogo 665-0852 (JP). NISHIO, Toshiro [JP/JP]; 89-11, Higashifunabashi 1-chome, Hirakata-shi, Osaka 573-1115 (JP). SUZUKI, Hidekazu [JP/JP]; 469-1, Tsutsui-cho, Yamatokooriyama-shi, Nara 639-1123 (JP).

(74) Agent: NAKAJIMA, Shiro; 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 531-0072 (JP).

(81) Designated States *(national)*: CN, US.

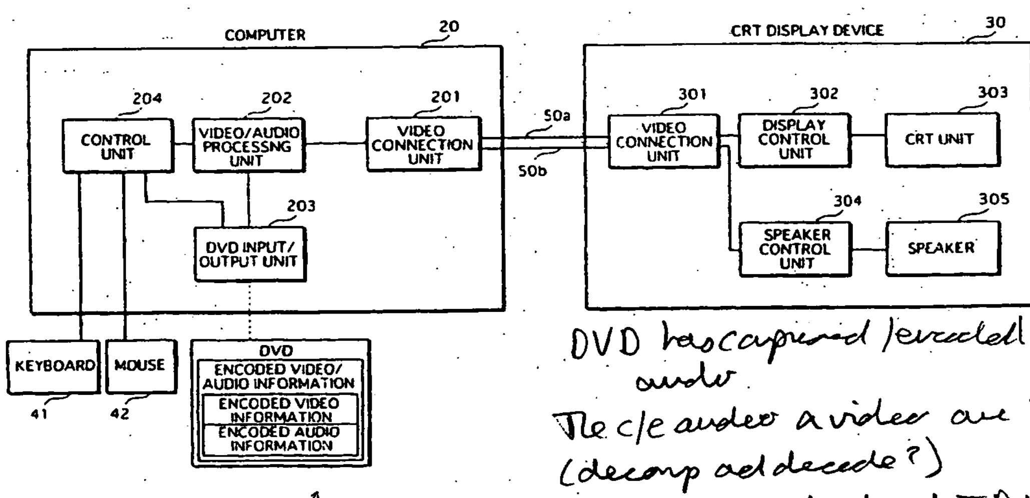
(84) Designated States *(regional)*: European patent (DE, FR, GB).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ENCRYPTION TRANSMISSION SYSTEM

see p9, p10



DVD has compressed/encoded video and audio
The c/e audio & video are 'decoded' (decomp and decode?)
Then encrypted and TDMd?

(57) Abstract: A video signal and an audio signal are time division multiplexed, encrypted, and transmitted. A transmission side time-compresses the audio signal, multiplexes, encrypts, and transmits the time-compressed audio signal in a blanking period of the video signal. Control is performed using an audio signal data enable signal ADE, and a audio signal/video signal switch signal.

WO 02/51150 A2

So irrelevant.

DESCRIPTION

ENCRYPTION TRANSMISSION SYSTEM

Technical Field

The present invention relates to an encryption transmission system that encrypts digital video signals and audio signals, and transmits the encrypted signals.

Background Art

When an analog signal is transmitted to an LCD (Liquid Crystal Display Device), a CRT (Cathode Ray Tube), or the like, distortions in the wave form and the like generate blurring and ghosting on the display screen.

DVI specification

In order to solve the above-described problem, in the DVI (Digital Visual Interface) Standard, video signals are sent digitally to LCDs, CRTs, and the like. This enables a screen to be displayed with high picture quality and without distortion.

Conventional signal transmission systems to which the DVI specification is applied are composed of a transmission device and a reception device which are connected via a transmission

path. The transmission device has three TDMS (Transition Minimized Differential Signaling) encoders/serializers, and the reception device has three TDMS recovery/decoders. Component signals of each of RED, GREEN, and BLUE are input into the respective corresponding TDMS encoder/serializers, encoded therein, and the results serialized and output to the transmission path. Next, each of the TDMS recovery/decoder in the reception device decodes the respective received signal, and recovers and reconstructs the respective component signal.

A DE (data enable) signal shows a period in which component signals RED, GREEN, BLUE, etc. exist, and is HIGH active. A period in which the DE signal is LOW is, for example, a horizontal synchronization signal period or a vertical synchronization signal period. CLT signals CTL0, CLT1, CTL2, and CLT3 are provided as control signals, but in the current DVI specification these signals are unused. Specifically, ordinarily the level of these signals is zero.

Each of the TMDS encoder/serializers in the transmission device converts an input 8-bit signal into 10 bits, and serializes and sends the converted 10-bit video signal in serial to the transmission path. The purpose of converting from 8 bits to 10 bits is that a 10-bit signal is suitable for high-speed transmission of data with fewer data change points. In addition, the TDMS encoder/serializers convert the 2-bit control signal

to 10 bits and transmit the result to the transmission path. The data enable signal is also encoded, serialized and transmitted to the transmission path. The TDMS recovery/decoders in the reception device decode and expand the 10-bit serial data received from the transmission path into 8-bit color signals, a 2-bit data enable signal, and a 2-bit control signal.

HDCP specification

An HDCP (High-bandwidth Digital Content Protection System) specification has been proposed as a digital content protection system that is compatible with the DVI specification.

The HDCP specification uses a signal transmission system that is compatible with the DVI specification to transmit video content requiring right protection. Essentially the HDCP specification consists of authentication between the transmission device and the reception device, sharing of a key, and encryption of video content over a communication path.

A transmission device in a signal transmission system that complies with the HDCP specification has an authentication unit that performs authentication and key exchange with the reception unit, an encryption unit that encrypts video information using a shared key, and a TMDS encoding unit. A

reception unit has an authentication unit that performs authentication and key exchange with the transmission unit, a TDMS decoding unit, and a decryption unit that decrypts a received signal using the shared key.

According to this construction, after verification and key exchange via an I^2C between the transmission device and the reception device, the transmission device encrypts video RGB data, and transmits the encrypted data via a TDMS encoder that complies with the DVI specification. After receiving the encrypted data via a TMDS decryption unit that complies with the DVI specification, the reception unit decrypts the encrypted video RGB data using the same key as that used by the transmission device, to obtain the original video RGB signal. In the HDCP specification the encryption used here is called "HDCP Cipher". The core part of HDCP Cipher is common to authentication, key exchange, and video data encryption.

As explained above, a data transmission system that is compatible with DVI specifications and HDCP specifications enables transmission of high quality images while ensuring protection of right protected works over the transmission path.

In recent years it has become common to reproduce digital video to which digital audio is attached in personal computers, digital broadcast reception devices, DVD (Digital Versatile Disk) reproduction devices, and the like. Accordingly, there

is now a demand for high-quality transmission of audio, similar to that described above for video.

Disclosure of Invention

In order to responds to the aforementioned demands, the object of the present invention is to provide a transmission system, a transmission device, a reception device, a video generation device, and a video display device that are capable of transmitting video information and audio information with high quality.

In order to achieve the above described object, the present invention is a transmission system including: a transmission device and a reception device, the transmission device transmitting digital video information while providing one or more blanking intervals during transmission of the digital video information, and the reception device receiving the digital video information, wherein the transmission device transmits digital audio information during the one or more blanking intervals, and the reception device receives the digital audio information during the one or more blanking intervals.

According to the above-described transmission system, video information and audio information can be transmitted with high picture quality.

Furthermore, the present invention is a transmission system including: a video transmission device and a video display device, the video transmission device encrypting and transmitting frame information that includes digital video information while providing one or more blanking intervals during the frame information, and the video display device receiving and decrypting the encrypted frame information, extracting the digital video information from the decrypted frame information, and displaying the extracted video information, wherein in the one or more blanking intervals the video transmission device multiplexes digital audio information with the frame information, encrypts the multiplexed frame information with which the digital audio information has been multiplexed, and transmits the encrypted frame information, and the video display device receives the encrypted frame information, decrypts the received encrypted frame information to generate frame information, extracts the digital audio information from the one or more blanking intervals provided in the generated frame information, and converts the extracted digital audio information to an audio signal.

According to the above described transmission system, video information and audio information can be transmitted with high picture quality while being protected as right protected

works.

Brief Description of Drawings

Fig. 1 is an outline of a personal computer system 10;

Fig. 2 is a block drawing showing the structure of the personal computer system 10;

Fig. 3 is a block drawing showing the structure of a video connection unit 201 and a video connection unit 301;

Fig. 4 is an outline drawing showing the relationship between a vertical retrace period, a horizontal retrace period, and one frame of video information;

Fig. 5 shows changes in one frame of data enable signals DE and ADE, decoded video information, and encoded audio information, as time elapses;

Fig. 6 shows changes in one line of data enable signals DE and ADE, decoded video information, and encoded audio information, as time elapses;

Fig. 7 is a block drawing showing the structure of a TMDS encoding unit 213 and a TDMS decoding unit 311;

Fig. 8 is a flowchart showing an overview of the operation of the personal computer system 10 when reproducing encoded video/audio information;

Fig. 9 is a flowchart showing device authentication operations;

Fig. 10 is a flowchart showing key exchange operations for each frame;

Fig. 11 is a flowchart showing audio information and video information encryption, transmission and decryption, in one line; and

Fig. 12 is a transition chart showing state transition in encrypting [decrypting] by an HDCP encryption unit 215 [HDCP decryption unit 315].

Best Mode for Carrying Out the Invention

The following describes a personal computer system 10 as a first embodiment of the present invention.

1. Structure of the personal computer system 10

As shown in Fig. 1, the personal computer system 10 is composed of a computer 20, a CRT display device 30, a keyboard 41, and a mouse 42. The main body 20 and the CRT display device 30 are connected by cables 50a and 50b.

Furthermore, as shown in Fig. 2, the computer 20 is composed of a video connection unit 201, a video/audio processing unit 202, a DVD input/output unit 203, a control unit 204, and other units that are not illustrated. The computer 20 also includes a microprocessor, a ROM (read only memory), a RAM (random access memory), a hard disk unit, and so on.

Computer programs are stored in the RAM and the hard disk unit. The main body 20 performs its functions according to operations of the microprocessor following the computer programs.

The CRT display device 30 is composed of a video connection unit 301, a display control unit 302, a CRT unit 303, a speaker control unit 304, and speakers 305.

As shown in Fig. 3, the video connection unit 201 is composed of a multiplex unit 211, an HDCP encryption unit 215, and a TDMS encoding unit 213. The HDCP encryption unit 215 includes an encryption unit 212 and an authentication key exchange unit 214. As shown in Fig. 3, the video connection unit 301 is composed of a TMDS decoding unit 311, an HDCP decryption unit 315 and a separation unit 313. The HDCP decryption unit 315 includes an encryption unit 312 and an authentication key exchange unit 314.

The DVD stores encoded video/audio information composed of encoded video information and encoded audio information. Here, the encoded video information is video information that has been compressed and encoded, while the encoded audio information is audio information that has been compressed and encoded. One example of the audio/video information is movie information composed of moving images and audio information. The DVD is placed in the DVD input/output unit 203 by a user.

The computer 20 reads encoded video/audio information

from the DVD that has been placed in computer 20, and separates the read encoded video/audio signal to generate the encoded video information and the encoded audio information. Next, the computer 20 decodes the encoded video information to generate decoded video information. Here, the decoded video information and the encoded audio information are digital signals. Next, the computer 20 encrypts the decoded video information and the encoded audio information to generate encrypted video information and encrypted audio information respectively. The computer 20 then outputs the generated encrypted video information and the generated encrypted audio information via the cable 50a to the CRT display device 30. The CRT display device 30 decrypts the received encrypted video information and the received encrypted audio information to generate decrypted video information and decrypted audio information, displays the generated decrypted video information on the CRT unit 303, and converts the generated decrypted audio information to an analog signal which is output by the speakers 305.

Does this mean also decompress ? possibly yes.

1.1 Keyboard 41, mouse 42, control unit 204, DVD input/output unit 203, and video/audio processing unit 202

The keyboard 41 and the mouse 42 receive an instruction from the user to reproduce the encoded video/audio information

recorded on the DVD, generate instruction information corresponding to the received instruction, and output the generated instruction information to the control unit 204.

The control unit 204 receives the instruction information, and outputs an instruction, based on the received instruction information, to the DVD input/output unit 203 to read the encoded video/audio information.

The DVD input/output unit 203 receives the read instruction, reads the encoded video/audio information from the DVD based on the received read instruction, and outputs the read encoded video/audio information to the video/audio processing unit 202.

The video/audio processing unit 202 receives the encoded video/audio information which it separates to generate the encoded video information and the encoded audio information. Then the video/audio processing unit 202 decodes the generated encoded video information to generate decoded video information, and outputs the generated decoded video information and the generated encoded audio information to the video connection unit 201.

1.2 Video connection unit 201.

(1) Multiplex unit 211

The multiplex unit 211 receives decoded video information

and encoded audio information.

The decoded video information includes a plurality of pieces of frame video information, each of which corresponds to one frame. Moving images are expressed by displaying the plurality of pieces of frame video information in succession on the CRT display device 30. Each piece frame video information includes 480 pieces of line video information which together corresponds to one line.

The encoded audio information includes frame audio information that corresponds to the frame video information. The frame audio information is converted into audio and output in the time slot in which the corresponding frame video information is being reproduced in the CRT display device 30. Each piece of frame audio information includes 480 pieces of line audio information that correspond to the pieces of line video information.

The multiplex unit 211, when transmitting one piece of frame video information from amongst the decoded video information from the main body 20 to the CRT display device 30, provides a vertical retrace period (also called a "vertical blanking interval") directly before the frame video information is transmitted. This is for establishing synchronization between the main body 20 and the CRT display device 30 for displaying the frame video information. Here, the vertical

retrace period includes a time at which a predetermined number of vertical synchronization signals are transmitted. Next, the multiplex unit 211 provides a horizontal retrace period (also called a "horizontal blanking interval") directly before transmitting the pieces of line video information. This is for establishing synchronization for displaying the pieces of line video information included in each piece of frame video information. Here, the horizontal retrace period includes a time at which a horizontal synchronization signal is transmitted.

Fig. 4 shows the relationship between the vertical retrace period, the horizontal retrace period, and one piece of frame video information. As shown in the figure, each piece of frame video information is composed of 480 pieces of line video information, and each piece of video line information is composed of 720 pixels. Furthermore, each pixel has 24 bits, the 24 bits including 8-bit component information for each of RED, GREEN, and BLUE. As shown in the figure, the multiplex unit 211 provides, as a vertical retrace period, a time slot as a vertical retrace period directly before transmitting the piece of frame video. This time slot is equivalent to transmitting 45 pieces of line video information. Next, the multiplex unit 211 provides, as a horizontal retrace period, a time slot directly before transmitting each piece of line

video information. This time slot is equivalent to transmitting 138 pixels.

As shown in Fig. 5, at the starting point of the vertical retrace period the multiplex unit 211 sets, for each piece of frame video information from amongst the received pieces of decoded video information, both a data enable signal DE for the video signal and a data enable signal ADE for the audio signal to LOW. The multiplex unit 211 outputs the data enable signals DE and ADE that have been set to LOW to the TDMS encoding unit 213.

Next, in the vertical retrace period, the multiplex unit 211 sets the audio signal data enable signal ADE to HIGH from a point at which the HDCP encryption unit 215 has completed calculating a frame key (explained later), and outputs the data enable signal ADE set to HIGH to the TMDS encoding unit 213. The multiplex unit 211 also starts outputting the encoded audio signal from the point at which the HDCP encryption unit 215 has completed calculating the frame key.

Fig. 5 shows how the data enable signals DE and ADE, the decoded video information, and the encoded audio information in one time slot in which one piece of frame video data information is transmitted vary over time. In this figure time elapses from left to right along a line 401, then from left to right along a line 402, and so on in the same manner along lines

403, 404,..., and 405.

The time slot shown by the lines 401, 402,..., 403 is the vertical retrace period.

In the time slot shown by the line 401, the multiplex unit 211 sets the data enable signal DE to LOW, and sets the data enable signal ADE to LOW. The multiplex unit 211 does not output decoded video information or encoded audio information in this time slot. Furthermore, at the starting point of the time slot shown by the line 401, calculation of the frame key by the HDCP encryption unit 215 begins.

Likewise, at the starting point of the time slot shown by the line 402 the multiplex unit 211 sets the data enable signals DE and ADE to LOW. Next, in the time slot shown by the line 402, supposing that the calculation of the frame key by the HDCP encryption unit 215 has been completed, the multiplex unit 211 sets the audio signal data enable signal ADE to HIGH from the point at which the calculation of the frame key is completed, and outputs the data enable signal ADE set to HIGH to the TMDS encoder 213. The multiplex unit 211 also starts outputting one piece of audio information from the point at which the calculation of the frame key has been completed.

In the time slot shown from the next line after the line 402 to the line 403, the multiplex unit 211 sets the data enable signal DE to LOW, sets the audio signal data enable signal ADE

to HIGH, and outputs the data enable signals DE and ADE to the TMDS encoding unit 213. Furthermore, the multiplex unit 211 continues to output the piece of line video information.

Next, in the time slot shown by the line 404 the multiplex unit 211 sets the data enable signal DE to LOW for the time slot that corresponds to the horizontal retrace period, and outputs the data enable signal DE set to LOW to the TMDS encoding unit 213. Next, for the period for one piece of line video information that starts directly after the horizontal retrace period has ended, the multiplex unit 211 sets the data enable signal DE to HIGH, and outputs the data enable signal DE set to HIGH to the TMDS encoding unit 213.

Furthermore, in the time slot shown by the line 404 the multiplex unit 211 sets, in the horizontal retrace period, the audio signal data enable signal ADE to HIGH, outputs the data enable signal ADE set to HIGH, and continues to output the piece of line audio information to the encryption unit 212. Here, the piece of line audio information continuously output in the lines 402 to 404 is composed of a number of audio cells that is determined according to the point at which the HDCP encryption unit 215 completed calculating the frame key. Each audio cell is composed of encoded audio information that is 24 bits long. Furthermore, in the period starting directly after the horizontal retrace period ends the multiplex unit 211

outputs a piece of line video information to the encryption unit 212. Here, a piece of line video information is composed of 720 pixels.

Fig. 6 shows the relationship in the time slots in the next line after the time slot shown by the line 404 to the time slot shown by the line 405 between the data enable signals DE and ADE, the encoded audio information, and the decoded video information. As shown in the figure, the multiplex unit 211 outputs a piece of line audio information to the encryption unit 212 in the horizontal retrace period. Here, the piece of line audio information is composed of 138 audio cells. Each audio cell is composed of a piece of encoded audio information that is 24 bits long. In addition, the multiplex unit 211 outputs one piece of line video information to the encryption unit 212 in the period that starts directly after the horizontal retrace period has ended. Here, the one piece of line video information is composed of 720 pixels.

In addition, the multiplex unit 211, in the vertical retrace period, generates a predetermined number of vertical synchronization signals VSYNC, and outputs the generated vertical synchronization signals VSYNC to the TMDS encoding unit 213. Furthermore, the multiplex unit 211, in the horizontal retrace period, generates a horizontal synchronization signal HSYNC, and outputs the generated

horizontal synchronization signal HSYNC to the TMDS encoding unit 213.

(2) Authentication key exchange unit 214

The authentication key exchange unit 214 operates following the HDCP specification. The main operation of the authentication key exchange unit 214 is to generate random numbers for device authentication, key exchange, and encryption between the authentication key exchange unit 214 and the device on the reception side. Details regarding the authentication key exchange unit 214 are specified by the HDCP specification and are thus omitted here.

The authentication key exchange unit 214 is connected via the cable 50b, which is an I^2C bus, to an authentication key exchange unit 314 that is described later.

Note that functions and structure unique to the authentication key exchange unit 214 of the present embodiment are described later.

(3) Encryption unit 212

Each clock cycle the encryption unit 212 receives a pixel and an audio cell from the multiplex unit 212, and receives a random number PRj from the authentication key exchange unit 214.

Next, on receiving a pixel, the encryption unit 212

performs exclusive OR on the received pixel and random number PRj one bit at a time to generate an encrypted pixel, and outputs the generated encrypted pixel to the TMDS encryption unit 213. This exclusive OR operation is shown by Expression 1.

<Expression 1>

encrypted pixel = pixel (+) random number PRj

Here, the operator (+) shows exclusive OR.

Likewise, on receiving an audio cell, the encryption unit 212 performs exclusive OR on the received audio cell and random number PRj one bit at a time to generate an encrypted audio cell, and outputs the generated encrypted audio cell to the TMDS encoding unit 213. This exclusive OR operation is shown by Expression 2.

<Expression 2>

encrypted audio cell = audio cell (+) random number PRj

(2) TDMS encoding unit 213

The TDMS encoding unit 213 is connected via the cable 50a to a TDMS decoding unit 311 that is described later.

As shown in Fig. 7, the TMDS encoding unit 213 is composed of TMDS encoder/serializers 213a, 213b, and 213c which are

connected respectively via channels C12, C11, and C10 in the cable 50a, to TMDS recovery/decoders 311a, 311b, and 311c that are described later.

TMDA encoder/serializer 213a

The TMDS encoder/serializer 213a receives RED component information of an encrypted pixel, and the first 8 bits of an audio cell, from the encryption unit 212. In addition, the TMDS encoder/serializer 213a receives a data enable signal DE for video information, a data enable signal ADE for audio information, and other control signals, from the multiplex unit 211.

The TMDS encoder/serializer 213a TDMS encodes the received 8-bit RED component information, the first 8 bits [23:16] of the audio cell, the data enable signal DE, the data enable signal ADE, and the other control signals, serializes the result, and sends the serialized result via the channel C12 to the TMDS recovery/decoder 311a.

In more detail, the TMDS encoder serializer 213a converts the 8-bit RED component information and the first 8 bits [23:16] of the audio cell both to 10-bit information, serializes the pieces of 10-bit information, and sends the result. By converting from 8 bits to 10 bits information that is more suitable for high-speed transmission with fewer data change

points is obtained. The TMDS encoder/serializer 213a also coverts both the data enable signals DE and ADE, which are the 2-bit control signals, into 10 bits, and sends the converted signals.

TMDS encoder/serializer 213b

The TMDS encoder/serializer 213b receives the GREEN component information of the encrypted pixel, and the middle 8 bits [15:8] of the audio cell, from the encryption unit 212. The TMDS encoder/serializer 213b also receives the data enable signal DE for the video signal, and other control signals, from the multiplex unit 211.

The TMDS encoder/serializer 213b encodes, in the same manner described above, the received 8-bit GREEN component information, the middle 8 bits [15:8] of the audio cell, the data enable signal DE, and the other control signals, serializes the result, and sends the serialized result via the channel C11 to the TMDS recovery/decoder 311b.

TMDS encoder/serializer 213c

The TMDS encoder/serializer 213c receives the BLUE component information of the encrypted pixel, and the end 8 bits [0:7] of the audio cell, from the encryption unit 212. The TMDS encoder/serializer 213b also receives the data enable signal

DE for the video signal, the vertical synchronization signal VSYNC, and the horizontal synchronization signal HSYNC, from the multiplex unit 211.

The TMDS encoder/serializer 213c encodes, in the same manner described above, the received 8-bit BLUE component information, the end 8 bits [0:7] of the audio cell, the data enable signal DE, the vertical synchronization signal VSYNC, and the horizontal synchronization signal HSYNC, serializes the result, and sends the serialized result via the channel C10 to the TMDS recovery/decoder 311c.

1.3 Video connection unit 301

(1) TMDS decoding unit 311

As shown in Fig. 7, the TMDS decoding unit 311 is composed of TMDS recovery/decoders 311a, 311b, and 311c.

TMDS recovery/decoder 311a

The TMDS recovery/decoder 311a receives the serial data from the TDMS encoding unit 213 via the channel C12, and decodes from the received serial data the 8-bit RED component information, the first 8 bits [23:16] of the audio cell, the data enable signal DE, the data enable signal ADE, and the other control signals. The TMDS recovery/decoder 311a outputs the 8-bit RED component information, and the first 8 bits [23:16]

of the audio cell to the encryption unit 312, and outputs the data enable signal DE, the data enable signal ADE, and the other control signals to the separation unit 313.

TMDS recovery/decoder 311b

The TMDS recovery/decoder 311b receives the serial data from the TDMS encoding unit 213 via the channel C12, and decodes from the received serial data the 8-bit GREEN component information and the middle 8 bits [15:8] of the audio cell, and outputs the decoded result to the encryption unit 312.

TMDS recovery/decoder 311c

The TMDS recovery/decoder 311c receives the serial data from the TDMS encoding unit 213 via the channel C10, and decodes from the received serial data the 8-bit BLUE component information, the end 8 bits [7:0] of the audio cell, the vertical synchronization signal VSYNC, and the horizontal synchronization signal HSYNC. The TMDS recovery/decoder 311c outputs the 8-bit BLUE component information, and the end 8 bits [7:0] of the audio cell to the encryption unit 312, and outputs the vertical synchronization signal VSYNC, and the horizontal synchronization signal HSYNC to the display control unit 302.

(2) Authentication key exchange unit 314

The authentication key exchange unit 314 operates following HDCP specifications, as does the authentication key exchange unit 214. The main operation of the authentication key exchange unit 314 is to generate random numbers for device authentication, key exchange, and encryption between the authentication key exchange unit 314 and the device on the transmission side. Details regarding the authentication key exchange unit 314 are specified by HDC specifications and are thus omitted here.

Note that functions and structure unique to the authentication key exchange unit 314 of the present embodiment are described later.

(3) Encryption unit 312

The encryption unit 312 operates in the same way as the encryption unit 212.

Each clock cycle the encryption unit 312 receives an encrypted pixel and an encrypted audio cell form the TMDS decoding unit 311, and receives a random number PRj from the authentication key exchange unit 314.

Next, on receiving a pixel, the encryption unit 312 performs exclusive OR on the received encrypted pixel and random number PRj one bit at a time to generate a decrypted pixel, and outputs the generated decrypted pixel to the separation unit

313. This exclusive OR operation is shown by Expression 3.

<Expression 3>

decrypted pixel = encrypted pixel (+) random number PRj

Here, the random number used to generate the encrypted pixel in Expression 1 and the random number used to generate the decrypted pixel in Expression 3 have the same value, therefore the original pixel is obtained as a result of the decryption.

Likewise, on receiving an encrypted audio cell, the encryption unit 312 performs exclusive OR on the received encrypted audio cell and random number PRj one bit at a time to generate an decrypted audio cell, and outputs the generated decrypted audio cell to the separation unit 313. This exclusive OR operation is shown by Expression 4.

<Expression 4>

decrypted audio cell = encrypted audio cell (+) random number PRj

Here, the random number used to generate the encrypted audio cell in Expression 2 and the random number used to generate the decrypted audio cell in Expression 4 have the same value,

therefore the original audio cell is obtained as a result of the decryption.

(4) Separation unit 313

Each clock cycle, the separation unit 313 receives 24-bit length information from the encryption unit 312, and a data enable signal DE and a data enable signal ADE from the TMDS decoding unit 311.

When the received data enable signal DE is HIGH, the separation unit 313 considers the received 24-bit data to be a decrypted pixel, and each clock cycle outputs the received 24-bit information to the display control unit 302. The separation unit 313 also outputs the data enable signal DE to the display control unit 302.

When the received data enable signal ADE is HIGH, the separation unit 313 considers the received 24 bit data to be a decrypted audio cell, and each clock cycle outputs the received 24-bit information to the speaker control unit 304. The separation unit 313 also outputs the data enable signal ADE to the speaker control unit 304.

1.4 Display control unit 302 and CRT unit 303

The display control unit 302 receives a decrypted pixel and a data enable signal DE from the separation unit 313 each

clock cycle, and receives a vertical synchronization signal VSYNC and a horizontal synchronization signal HSYNC from the TMDS decryption unit 311.

The display control unit 302 generates RED, GREEN, and BLUE analog signals based on the decrypted pixel, the data enable signal DE, the vertical synchronization signal VSYNC and the horizontal synchronization signal HSYNC received every clock cycle, and outputs each generated analog signal to the CRT unit 303.

The CRT unit 303 receives the RED, GREEN, and BLUE analog signals from the display control unit 302, and displays a color image.

1.5 Speaker control unit 304 and speakers 305

The speaker unit 304 receives a decrypted audio cell and a data enable signal ADE from the separation unit 313 each clock cycle. While the received data enable signals ADE are HIGH, the speaker unit 304 decodes the received decrypted audio cell to generate audio information, converts the generated audio information to generate an analog signal, and outputs the generated analog signal to the speakers 305.

The speakers 305 receives the analog signal from the speaker control unit 304, covert the received analog signal to generate audio, and output the generated audio.

2. Operations of the personal computer system 10

The following describes the operations of the personal computer system 10.

(1) Overview of operations of personal computer system 10

An overview of the operations of the personal computer system 10 when reproduction of audio/video information recorded on a DVD is instructed by the user is given with reference to the flowchart in Fig. 8.

Authentication is performed between the computer 20 and the CRT display 30 based on the HDCP specification. Here, the computer 20 verifies whether the CRT display device 30 is legitimate (step S101), and when the authentication fails (step S102) the process ends.

When the authentication succeeds (step S102), the computer 20 generates a KSV list based on the HDCP specification (step S103). Note that the HDCP specification describes KSV list generation, thus a description is omitted here.

Next, the computer 20 sets a value of a variable i showing a frame number to "0".

Then, the processing shown in steps S105 to S111 is repeated at steps S105 to S112 for each frame,.

The computer 20 adds 1 to the value of the variable i (step S106), and performs key exchange each frame (step S107). Next, at steps S108 to S111, steps S109 to S110 are repeated for each line.

Encryption, transmission, and decryption of one piece of line audio information and one piece of line video information are performed (step S109), and the key is updated based on HDCP specifications (step S110).

(2) Device authentication operations

The device authentication operations shown by step S101 in Fig. 8 are described using the flowchart shown in Fig. 9. Note that device authentication is described in the HDCP specification, thus a detailed description is omitted.

The authentication key exchanging unit 214 generates an An (step S171), and transmits the An and the Aksv via the cable 50b, which is an I^2C bus, to the authentication key exchange unit 314 (step S172).

The authentication key exchange unit 314 transmits the Bksv and the REPEATER via the cable 50b to the authentication key exchange unit 214 (step S173).

The authentication key exchange unit 214 calculates Km = Akeys over Bksv (step S174), and calculates (Ks, M_0, R_0) = dviBlkCipher (Km, REPEATER||An) (step S175).

The authentication key exchange unit 314 calculates Km' = Bkeys over Aksv (step S176), calculates (Ks', M_0', R_0') = dviBlkCipher (Km', REPEATER||An) (step S177), and transmits R_0' via the cable 50b to the authentication key exchange unit 214 (step S178).

The authentication key exchange unit 214 compares R_0 and R_0', and when the two are identical (step S179), recognizes the CRT display device 30 as being a legitimate device. When R_0 and R_0' are not identical (step S179), the authentication key exchange unit 214 recognizes the CRT display device 30 as not being a legitimate device.

(3) Key sharing operations for each frame

The following describes the operations shown by step S107 in Fig. 8, with use of the flowchart shown in Fig. 10. Note that key exchange for each frame is described in the HDCP specification, thus a detailed description is omitted.

The authentication key exchange unit 214 calculates (Ki, Mi, Ri,) = dviBlkCipher (Ks, REPEATER||Mi-1) (step S131). Next, the authentication key exchange unit 214, only when (i mod 128) is "0" (step S132), calculates Ri=ri (step S133).

The authentication key exchange unit 314 calculates (Ki', Mi', Ri') = dviBlkCipher (Ks', REPEATER||M'i-1) (step S141). Next, the authentication key exchange unit 314 only when (i mod

128) is "0" (step S142), calculates Ri'=ri' (step S143). Next, the authentication key exchange unit 314 transmits Ri' every two seconds via the cable 50b to the authentication key exchange unit 214.

The authentication key exchange unit 214 compares Ri and Ri' every two seconds, and when Ri and Ri' are identical (step S135) recognizes the CRT display device 30 as being a legitimate device. When Ri and Ri' are not identical, the authentication key exchange unit 214 recognizes the CRT display device 30 as not being a legitimate device.

(4) Encryption, transmission, and decryption operations for one piece of line audio information and one piece of line video information

The following describes encryption, transmission, and decryption operations shown by step S109 in Fig. 8 for one piece of line audio information and one piece of line video information, with use of the flowchart in Fig. 11.

The authentication key exchange unit 214 temporarily saves, as a saved initial value, an initial value used in random numbers generation specified by the HDCP specification. Here, the initial value is specifically Mi-1 (step S200).

Next, at steps S201 to S205, the following steps S202 to S204 are repeated for each audio cell Acj in one piece of line

audio information. Here, there are 138 audio cells in one piece of line audio information. The variable j takes a value of 1 through to 138 in the aforementioned repetition of the steps S202 to s204.

The authentication key exchange unit 214 generates a 24-bit random number PRj (step S202), and the encryption unit 212 performs exclusive OR on the audio cell ACj and the random number PRj to generate an encrypted audio cell EACj (step S203). Next, the encryption unit 212 transmits the generated encrypted audio cell EACj to the encryption unit 312, via the TMDS encoding unit 213, the cable 50a, and the TMDS decoding unit 311 (step S204).

The authentication key exchange unit 314 temporarily saves, as a saved initial value, an initial value used in random number generation specified by the HDCP specification. Here, the initial value is specifically M'i-1 (step S221).

Next, at steps S222 to S225, the following steps S223, S204, and S224 are repeated for each encrypted audio cell DACj in one piece of line audio information. Here, there are 138 encrypted audio cells in one piece of line audio information. The variable j takes a value of 1 through to 138 in the aforementioned repetition of the steps S223, S204, and S224.

The authentication key exchange unit 314 generates a 24-bit random number PRj (step S223), and the encryption unit

312 performs exclusive OR on the encrypted audio cell DACj and the random number PRj to generate an decrypted audio cell DACj. Then the encryption unit 312 outputs the generated decrypted audio cell DACj to the separation unit 313 (step S224).

The authentication key exchange unit 214 restores the initial value from the temporarily stored saved initial value (step S206). Next, at steps S207 to S211 the following steps S208 to S211 are repeated for each pixel PCj in one piece of line video information. Here, there are 720 pixels in one piece of line video information. The variable j takes a value of 1 through to 720 in the aforementioned repetition of the steps S208 to S210.

The authentication key exchange unit 214 generates a 24-bit random number PRj (step S208), and the encryption unit 212 performs exclusive OR on the pixel PCj and the random number PRj to generate an encrypted pixel EPCj (step S209). Next, the encryption unit 212 transmits the generated encrypted pixel EPCj to the encryption unit 312, via the TMDS encoding unit 213, the cable 50a, and the TMDS decoding unit 311 (step s210).

The authentication key exchange unit 314 restores the initial value from the temporarily stored saved initial value (step S226). Next, at steps S227 to S230 the following steps S228, S210, and S229 are repeated for each encrypted pixel DPCj in one piece of line video information. Here, there are 720

pixels in one piece of line video information. The variable j takes a value of 1 through to 720 in the aforementioned repetition of the steps S228, S210, and S229.

The authentication key exchange unit 314 generates a 24-bit random number PRj (step S228), and the encryption unit 312 performs exclusive OR on the encrypted pixel EPCj and the random number PRj to generate an decrypted pixel DPCj. Then the encryption unit 312 outputs the generated decrypted pixel DPCj to the separation unit 313 (step S229).

(5) Encryption [decryption] by the HDCP encryption unit 215 [HDCP decryption unit 315]

The following describes state transition in encryption [decryption] by the HDCP encryption unit 215 [HDCP decryption unit 315], with use of Fig. 12. Note that the contents of square brackets denote state transition in decryption by the HDCP decryption unit 315.

<Transition from any state to idle state D0>

In the case of reset conditions (step s301), or authentication failure (step S304) the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to an idle state D0.

<Transition from idle state D0 to frame key calculation state D1>

The HDCP encryption unit 215 [HDCP encryption unit 315], based on HDCP specifications, uses the CTL 3 signal, which is unused in the DVI specification, as a synchronization signal for frame key calculation. When authentication is successful and a DVI interface CTL 3 signal has been generated (step S302), the HDCP encryption unit 215 [HDCP encryption unit 315] transitions to a frame key calculation state D1 for performing frame key calculation. In the frame key calculation state D1, the HDCP encryption unit 215 [HDCP decryption unit 315] calculates a frame key to be used in encrypting [decrypting] the next video frame.

<Transition from frame key calculation state D1 to video encryption [decryption] state D2>

During the vertical blank period, when there is no audio signal start signal, on receiving a DE signal that gives the top of a video signal to be encrypted [decrypted] (step S309), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to a video encryption [decryption] state D2. In the video encryption state D2, the HDCP encryption unit 215 [HDCP decryption unit 315] encrypts [decrypts] the video signal.

<Transition from video encryption [decryption] state D2 to unknown blank state D3>

The end of video data (generally the end of a line or the

end of a frame) is notified by DE. This signal is shown as "!DE" in Fig. 12. On receiving !DE, the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to an unknown blank state D3. In the unknown blank state D3, the HDCP encryption unit 215 [HDCP decryption unit 315] begins updating the key.

<Transition from unknown blank state D3 to frame key calculation state D1>

On receiving a CTL 3 signal in the unknown blank state D3 (step S303), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to the frame key calculation state D1 to calculate a key for the next video frame.

<Transition from unknown blank state D3 to horizontal blank state D4>

The assertion of the HSync identifies the horizontal blank (generally between lines). On receiving the HSync (step S310), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to an horizontal blank state D4.

In the horizontal blank state D4, the HDCP encryption unit 215 [HDCP decryption unit 315] waits if updating of the key has not been completed in the unknown blank state D3.

<Transition from the unknown blank state D3 to the vertical blank state D5>

The assertion of the VSync identifies the vertical blank (generally between frames). On receiving the VSync, the HDCP

encryption unit 215 [HDCP decryption unit 315] transitions to a vertical blank state D5.

<Transition from horizontal blank state D4 to video encryption [decryption] state D2>

On receiving a DE signal when there is no audio signal in the horizontal blanking period (step S314), the HDCP encryption unit 215 [HDCP decryption unit 315] begins encryption [decryption] of the next line of video signal, and transitions the video encryption [decryption] state D2.

<Transition from horizontal blank state D4 to frame key calculation state D1>

If a CTL signal 3 is generated (Step S315), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to the frame key calculation state D1 to calculate a key for the next frame.

<Transition from horizontal blank state D4 to vertical blank state D5>

The assertion of the VSync identifies the vertical blank. On receiving the VSync (Step S316) , the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to the vertical blank state D5.

In the vertical blank state D5, the HDCP encryption unit 215 [HDCP decryption unit 315] waits for an exit condition.

<Transition from vertical blank state D5 to frame key

calculation state D1>

If a CTL signal 3 is generated (Step S317), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to the frame key calculation state D1 to calculate a key for the next frame.

<Transition from vertical blank state D5 to idle state D0>

If there is a return according to a DE signal to a video signal in the vertical blank period before the CLT 3 signal is generated (step S319), the HDCP encryption unit 215 [HDCP decryption unit 315] does not encrypt the next frame. This may happen in link authentication failure.

<Transition from frame key calculation state D1 to audio encryption [decryption] state D6>

If there is a start signal ADE for an audio signal during the video blanking period (Step S305), the HDCP encryption unit 215 [HDCP decryption unit 315] begins encryption [decryption] of the audio signal.

In the audio signal encryption [decryption] state D6, the HDCP encryption unit 215 [HDCP decryption unit 315] encrypts [decrypts] the audio signal.

<Transition from audio encryption [decryption] state D6 to video signal wait state D7>

On being notified of the end of the audio signal according to the ADE (step S306), the HDCP encryption unit 215 [HDCP

decryption unit 315] transitions to a video signal wait state D7 where it waits for a video signal to start. In Fig. 12 this signal is expressed by "!ADE".

<Transition from video signal wait state D7 to video encryption [decryption] state D2>

The DE signal of the TDMS link gives the head of the video signal to be encrypted [decrypted]. On receiving the DE signal (step S307), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to the video encryption [decryption] state D2.

<Transition from horizontal blank state to audio encryption [decryption] state D8>

On receiving the ADE signal (step S311), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to an audio encryption [decryption] state D8 to begin encrypting [decrypting] the audio signal of the next horizontal blanking period.

In the audio encryption [decryption] state D8, the HDCP encryption unit 215 [HDCP decryption unit 315] encrypts [decrypts] the audio signal.

<Transition from audio encryption [decryption] state D8 to video signal wait state D9>

On being notified according to an ADE that the audio signal has ended (step S312), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to a video signal wait state

D9.

In the video signal wait state D9, the HDCP encryption unit 215 [HDCP decryption unit 315] waits for a video signal to start.

<Transition from video signal wait state D9 to video signal encryption [decryption] state D2>

The DE signal of the TMDS link gives the head of a video signal to be encrypted [decrypted]. On receiving the DE signal (step S313), the HDCP encryption unit 215 [HDCP decryption unit 315] transitions to the video encryption [decryption] state D2.

3. Conclusion

According to the above-described embodiment, in the encryption transmission system that performs encryption transmission by time division multiplexing of a video signal and an audio signal, the transmission side performs time-based compression of the audio signal, and performs encryption transmission by multiplexing the compressed audio signal in a video signal blanking period.

Furthermore, the transmission side of the encryption transmission system, after authentication with the reception side and after a vertical synchronization signal, calculates a key for the frame, and encrypts the time-compressed audio signal using the calculated key. Then the transmission side

encrypts the video signal, further updates the key, encrypts the next time-compressed audio signal using the updated key after a horizontal synchronization signal, and then encrypts the next video signal.

Furthermore, after authentication with the transmission side and after a vertical synchronization signal, the reception side of the encryption transmission system calculates the frame key, and decrypts the encrypted audio signal using the calculated frame key. Then the reception side decrypts the encrypted video signal, further updates the key, decrypts the next encrypted audio signal using the key that was updated after the horizontal synchronization signal, and then decrypts the next encrypted video signal.

Furthermore, the transmission side notifies the reception side of encrypted transmission of an audio signal with an audio signal enable signal, and notifies the reception side of encrypted transmission of a video signal with a video signal enable signal. Meanwhile, when there is an audio signal enable signal the reception side decrypts the audio signal, and when there is a video signal enable signal the reception side decrypts the video signal.

In this way, in the encryption transmission system, there is a data enable signal (ADE signal) for audio signals, in addition to the data enable signal (DA signal) for video signals

in the conventional example. These signals are controlled as a multiplex control signal. Since this ADE signal is added, the reception side is able to perform processing corresponding to the transmission side even if the audio signal is not multiplexed.

Furthermore, the encryption transmission system uses the same encryption method in encryption of the video signal and encryption of the audio signal in both the transmission side and the reception side.

Furthermore, when the encryption method has an internal state, the encryption transmission system sets an initial state to encrypt the audio signal, and then resets the encryption method internal state to its original initial value, and encrypts the next video signal.

The HDCP Cipher used in HDCP holds the internal state, and is an encryption method that depends on this internal state to input data, while updating the internal state. The transmission side saves the internal state of the encryption method at the state D3, and after audio signal processing (state D8), at state D9 returns the internal state to the saved state to perform encryption processing (state D2) of the next video signal. Therefore, even if the reception side device is an HDCP-compatible device that can only process video signals, the internal state of the encryption method is the same in both the

transmission side and the reception side when the video signal is decrypted (in other words, the transition from state D9 to state D2, and the transition from state D4 to state D2), thus the reception device can process the video signal correctly.

Furthermore, a common calculation module is used in authentication and key calculation in both the transmission side and the reception side, and in encryption of the video signal and the audio signal.

In this way, the encryption transmission system uses a common encryption algorithm for an audio signal and a video signal, therefore only minimum additions are required to a conventional encryption transmission system. In addition, a common calculation module is used in the same way as in HDCP in authentication and key sharing, and in encryption, therefore the scale of the system can be reduced.

Furthermore, the encryption transmission system multiplexes the video signal and the audio signal in the transmission side using a multiplex control signal, and separates these in the reception side using a multiplex control signal sent from the transmission side.

Furthermore, according to the present embodiment, the multiplex control signal is sent from the transmission side to the reception side, but it is possible to provide a non-signal period of a predetermined length between processing of an audio

signal and processing of a video signal, and have the reception side switch between audio signal and video signal by recognizing the non-signal period. In this way, in the encryption transmission system, instead of the multiplex control signal being sent by the transmission side to the reception side, the non-signal period is provided between the switch between the audio signal and the video signal, and the reception side generates a multiplex control signal when it recognizes this non-signal period.

As has been explained, according to the present embodiment, by expanding the state transition of the HDCP specification and the scale of the system as little as possible, not only can conventional video signals be encryption transmitted, but also audio signals that have been time-compressed in a blanking period can be multiplexed and encryption transmitted. An audio signal switching unit is added to the HDCP specification, and control is performed by an audio signal enable signal and a switch signal. This control means that the same processing as conventional HDCP specifications is possible when an audio signal is not multiplexed. Note that when the addition of a switch signal is difficult, switching can be performed by providing a non-signal period of a specified length in the data signal and having this non-signal period detected by the reception unit.

Furthermore, encryption transmission of a an audio signal with a video signal is possible while maintaining upward compatibility with the conventional HDCP specification and keeping expansion of the specification and the scale of the system to a minimum. Moreover, decryption and reproduction of an encrypted video signal are possible in a reception device that conforms to conventional HDCP specifications.

Furthermore, by using the same encryption method in encryption of an audio signal as in encryption of a video signal a compact scale with a minimum of extra modules is possible. In addition, by returning the internal state of the encryption method back to its initial value for each line after encryption of the audio signal of each line, video signals can be correctly decrypted even by a conventional HDCP specification-compatible reception device that does not comply to extended specifications, in other words that can only decrypt video signals.

4. Other Embodiments

The present invention is described based on, but is not limited to, the above-described embodiment. Cases such as the following are included in the present invention.

(1) The present invention is not limited to being implemented by a personal computer. The present invention may

be implemented in reproducing digital video to which digital audio is attached in a DVD (Digital Versatile Disk) reproduction device, a digital broadcast reception device, and the like.

(2) Although according to the present embodiment encoded audio information is transmitted to the video connection unit 301 from the video connection unit 201 via all of the channels C12, C11, and C10, it is possible to reduce the amount of encoded audio information that is transmitted, and transmit the encoded audio information via one or two of the channels.

Furthermore, transmission of encoded audio information from the video connection unit 201 to the video connection unit 301 is not limited to taking place in the vertical retrace period and horizontal retrace period, but may take place only in the vertical retrace period, or only in the horizontal retrace period.

(3) The present invention may be a method of any of the above-described embodiments. Furthermore, the present invention may be a computer program that implements any of the methods, and may be a digital signal that is composed of the aforementioned computer program.

Furthermore, the present invention may be the aforementioned computer program or the aforementioned digital signal recorded on a computer-readable recording medium such

as a flexible disk, a hard disk, a CD-ROM (compact disk read only memory), an MO (magneto-optical), a DVD, a DVD-ROM (digital versatile disk read only memory), a DVD-RAM (digital versatile disk random access memory), a semiconductor memory, and the like. Furthermore, the present invention may be the aforementioned computer program or the aforementioned digital signal recorded on any of the aforementioned recording mediums.

Furthermore, the present invention may be the aforementioned computer program or the aforementioned digital signal transmitted via an electric communication line, a wireless or wired communication line, a network of which the internet is representative, and the like.

Furthermore, the present invention may be a computer system that has a microprocessor and a memory, the memory storing the aforementioned computer program, and the microprocessor operating following the aforementioned computer program.

Furthermore, by recording and transferring the aforementioned program or the aforementioned digital signal on the aforementioned recording medium, or by transferring the aforementioned program or the aforementioned digital signal via the aforementioned network, the aforementioned program or the aforementioned digital signal may be implemented by another independent computer system.

(4) The present invention may be any combination of the above-described embodiment and the above-described variations.

Industrial Applicability

The present invention can be used in outputting video and audio in a personal computer, an information processing terminal, and the like. Furthermore, the present invention can also be used in outputting video and audio in a DVD reproduction device, a digital broadcast reception device, and the like.

Claims

1. A transmission system comprising:

a transmission device and a reception device,

the transmission device transmitting digital video information while providing one or more blanking intervals during transmission of the digital video information, and the reception device receiving the digital video information,

wherein the transmission device transmits digital audio information during the one or more blanking intervals, and the reception device receives the digital audio information during the one or more blanking intervals.

2. A transmission system comprising:

a video transmission device and a video display device,

the video transmission device encrypting and transmitting frame information that includes digital video information while providing one or more blanking intervals during the frame information, and the video display device receiving and decrypting the encrypted frame information, extracting the digital video information from the decrypted frame information, and displaying the extracted video information,

wherein in the one or more blanking intervals the video

transmission device multiplexes digital audio information with the frame information, encrypts the multiplexed frame information with which the digital audio information has been multiplexed, and transmits the encrypted frame information, and

the video display device receives the encrypted frame information, decrypts the received encrypted frame information to generate frame information, extracts the digital audio information from the one or more blanking intervals provided in the generated frame information, and converts the extracted digital audio information to an audio signal.

3. A video transmission device that transmits and encrypts frame information that includes digital video information, while providing one or more blanking intervals during the digital video information, the video transmission device, comprising:

multiplex means for multiplexing digital audio information with the frame information during the one or more blanking intervals;

encryption means for encrypting the frame information with which the digital audio information has been multiplexed; and

transmission means for transmitting the encrypted frame information.

4. The video transmission device of Claim 3

wherein the frame information includes, after a vertical blanking interval, a predetermined number of pieces of line video information after each of which a horizontal blanking interval is provided,

the digital audio information is composed of a plurality of pieces of line audio information, and

the multiplex means multiplexes the pieces of line audio information during the vertical blanking interval and/or the horizontal blanking intervals.

5. The video transmission device of Claim 4,

wherein the encryption means includes:

a frame key generation unit for generating a frame key that corresponds to the frame information, to be used as an encryption key; and

a frame encryption unit for encrypting, using the frame key generated corresponding to the frame information, the digital audio information and the digital video information included in the frame information.

6. The video transmission device of Claim 5

wherein the frame encryption unit includes:

a line encryption sub-unit for encrypting, using the frame key, one of the pieces of line audio information and one of the pieces of line video information included in the frame information;

a key updating sub-unit for updating the frame key; and

a repeat control sub-unit for controlling, until encryption of all of the pieces of line audio information and all of the pieces of line video information has finished, so that the line encryption sub-unit encrypts a next piece of line audio information and a next piece of line video information using the updated frame key, and controlling so that the key updating means updates the updated frame key again.

7. The video transmission device of Claim 5,

wherein the frame encryption unit uses a same encryption method in encrypting the digital audio information and the digital video information.

8. The video transmission device of Claim 7

wherein the line encryption sub-unit sets an initial value for audio, encrypts the line audio information using the set an initial value for audio, then sets an initial value for video to have a same value as the initial value for audio, and encrypts the line video information using the set initial value

for video.

9. The video transmission device of Claim 5 transmitting the encrypted frame information to a video display device,

wherein the encryption means uses a common calculation module in authentication of the video display device, in generating the frame key, and in encrypting the frame information.

10. The video transmission device of Claim 4

wherein the multiplex means further generates (a) a video enable signal that shows transmission of the digital video information, in a period in which the digital video information is included in the frame information, and (b) an audio enable signal that shows transmission of the digital audio information, in the blanking intervals, and

the transmission means further transmits the generated video enable signal and the generated audio enable signal.

11. The video transmission device of Claim 10

wherein the multiplex means generates the audio enable signal in the vertical blanking interval and/or the horizontal blanking intervals during which the digital audio information is multiplexed.

12. The video transmission device of Claim 3

wherein the multiplex means generates the frame information using a multiplex control signal that identifies transmission of the digital audio information and the digital video information, and

the transmission means transmits the multiplex signal.

13. The video transmission device of Claim 3

wherein the multiplex means generates frame information while providing a non-signal period between the digital audio information and the digital video information.

14. A video display device that receives the encrypted frame information from the video transmission device of Claim 3, decrypts the received frame information, extracts the digital video information from the decrypted frame information, and displays the extracted digital video information, the video display device comprising:

reception means for receiving the encrypted frame information;

decryption means for decrypting the encrypted frame information;

extraction means for extracting the decrypted digital

audio information from the blanking interval provided during the frame information, and extracting the digital video information from a period other than the one or more blanking intervals; and

output means for displaying the extracted digital video information, and converting the extracted digital audio information to audio.

15. The video display device of Claim 14

wherein the digital audio information includes a plurality of pieces of line audio information,

wherein the frame information includes, after a vertical blanking interval, a predetermined number of pieces of line video information after each of which a horizontal blanking interval is provided,

the plurality of pieces of line audio information are multiplexed in the vertical blanking interval and/or the horizontal blanking intervals, and

the extraction means extracts the pieces of line audio information from the vertical blanking interval and/or the horizontal blanking intervals.

16. The video display device of Claim 15

wherein the decryption means includes:

a frame key generation unit for generating a frame key that corresponds to the frame information, to be used as an decryption key; and

a frame decryption unit for decrypting, using the frame key generated corresponding to the frame information, the digital audio information and the digital video information included in the frame information.

17. The video display device of Claim 16

wherein the frame decryption unit further includes:

a line decryption sub-unit for decrypting, using the frame key, one of the pieces of line audio information and one of the pieces of line video information included in the frame information;

a key updating sub-unit for updating the frame key; and

a repeat control sub-unit for controlling, until decryption of all of the pieces of line audio information and all of the pieces of line video information has finished, so that the line decryption sub-unit decrypts a next piece of line audio information and a next piece of line video information using the updated frame key, and controlling so that the key updating means updates the updated frame key again.

18. The video display device of Claim 16

wherein the frame decryption sub-unit uses a same decryption method in decrypting the digital audio information and the digital video information.

19. The video display device of Claim 18

wherein the line decryption sub-unit sets an initial value for audio, decrypts the line audio information using the set initial value for audio, then sets an initial value for video to have a same value as the initial value for audio, and decrypts the line video information using the set initial value for video.

20. The video display device of Claim 16

wherein the decryption means uses a common calculation module in the authentication by the video display device, in generating the frame key, and in encrypting the frame information.

21. The video display device of Claim 15

wherein the transmission means further receives the video enable signal that shows transmission of the digital audio information, and the audio enable signal that shows transmission of the digital audio information, and

the extraction means further extracts the digital video

information in a period shown by the video enable signal, and extracts the digital audio information in a period shown by the audio enable signal.

22. The video display device of Claim 14

wherein the reception means receives a multiplex control signal that identifies transmission of the digital audio information and the digital video information, and

the extraction means extracts the digital audio information and the digital video information using the multiplex control signal.

23. The video display device of Claim 14

wherein the reception means receives encrypted frame information in which a non-signal period is provided between the digital audio information and the digital video information, and

the extraction means generates, using the non-signal period between the digital audio information and the digital video information, a multiplex control signal that identifies reception of the digital audio information and the digital video information, and extracts the digital audio information and the digital video information using the generated multiplex control signal.

FIG. 1

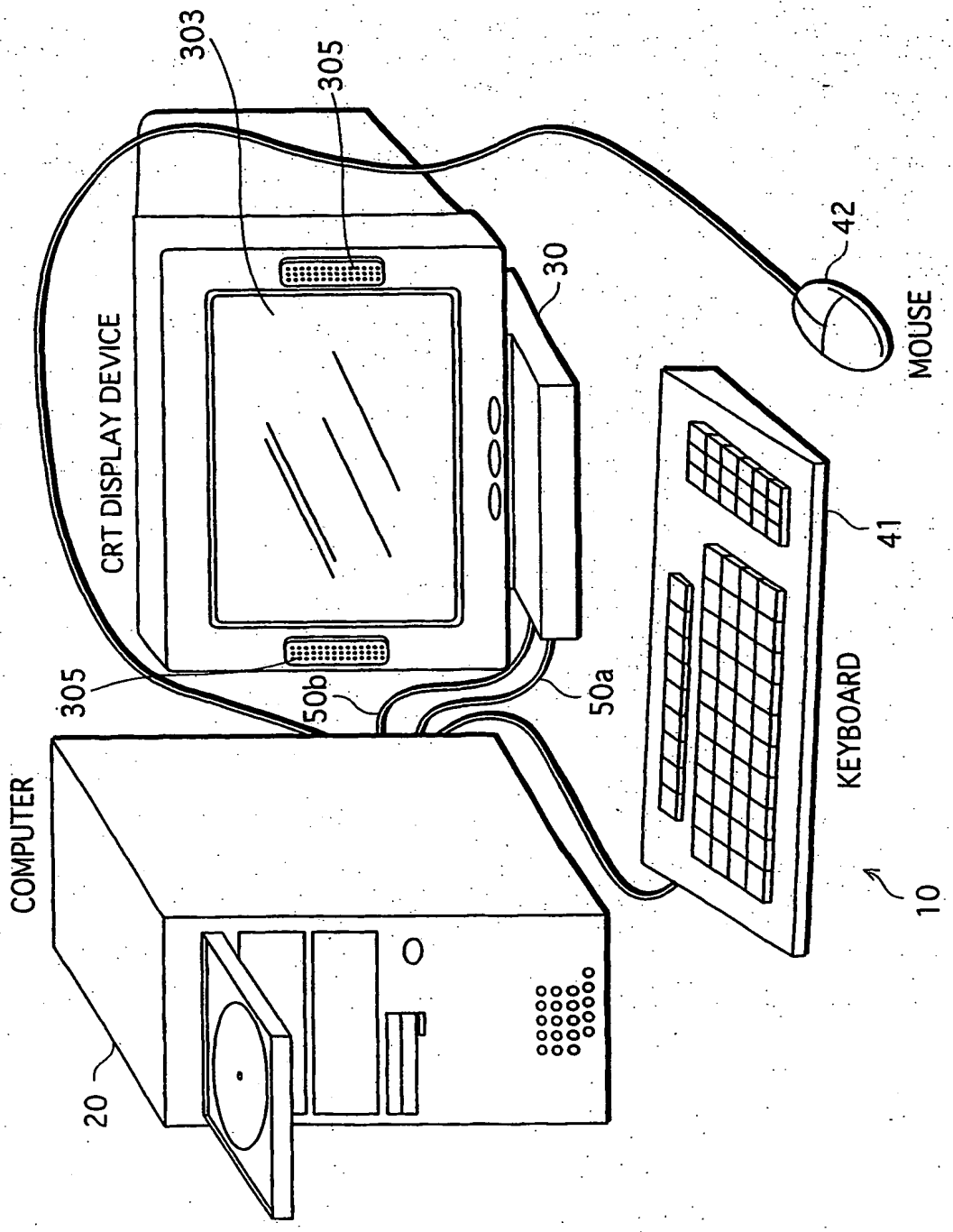

303
305
CRT DISPLAY DEVICE
30
42
MOUSE
41
KEYBOARD
305
50b
50a
COMPUTER
10
20

FIG.2

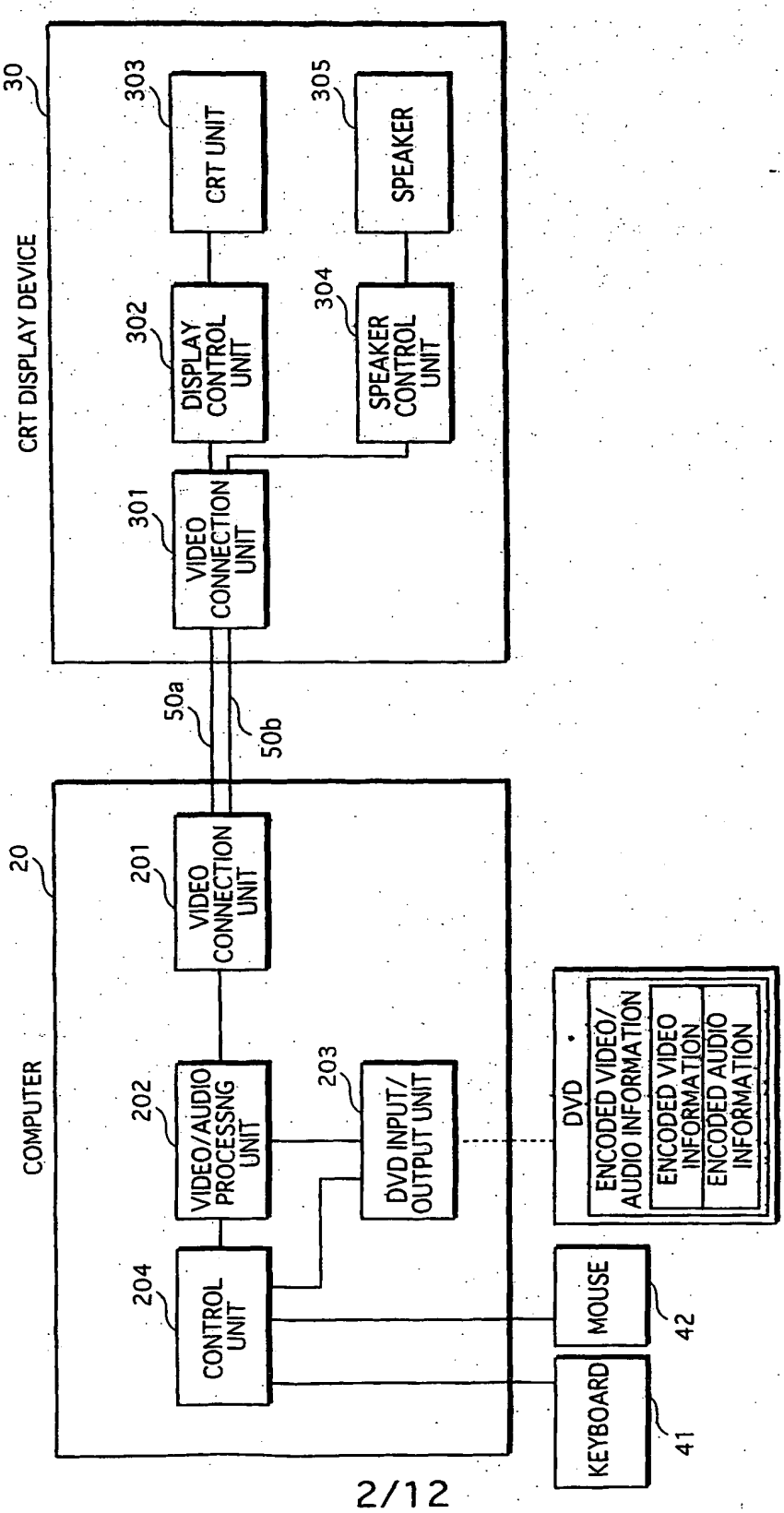

CRT DISPLAY DEVICE
30
303
CRT UNIT
305
SPEAKER
302
DISPLAY CONTROL UNIT
304
SPEAKER CONTROL UNIT
301
VIDEO CONNECTION UNIT
50a
50b
COMPUTER
20
201
VIDEO CONNECTION UNIT
202
VIDEO/AUDIO PROCESSNG UNIT
203
DVD INPUT/ OUTPUT UNIT
204
CONTROL UNIT
DVD
ENCODED VIDEO/ AUDIO INFORMATION
ENCODED VIDEO INFORMATION
ENCODED AUDIO INFORMATION
10
MOUSE
42
KEYBOARD
41

FIG.3

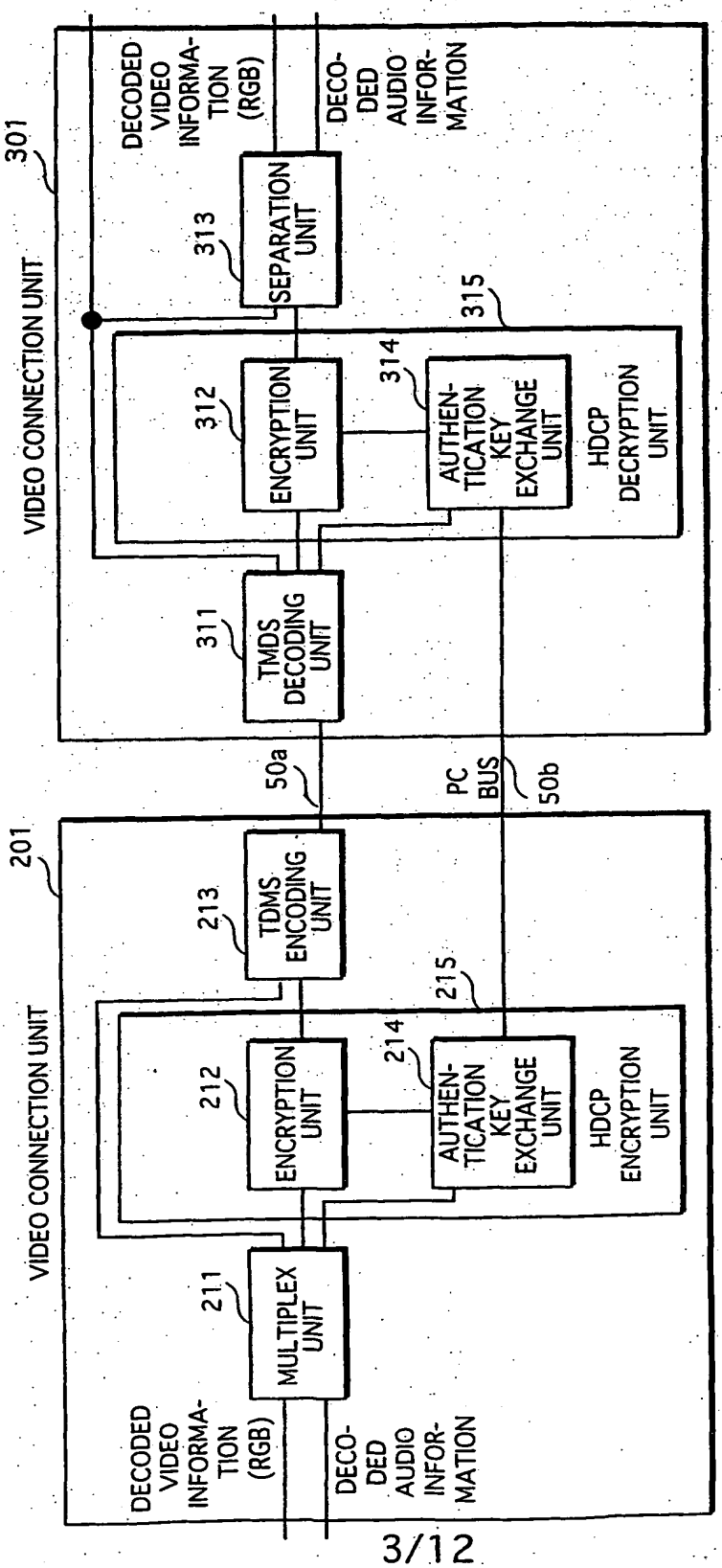

301
VIDEO CONNECTION UNIT
DECODED VIDEO INFORMATION (RGB)
DECODED AUDIO INFORMATION
313
SEPARATION UNIT
315
312
ENCRYPTION UNIT
314
AUTHENTICATION KEY EXCHANGE UNIT
HDCP DECRYPTION UNIT
311
TMDS DECODING UNIT
50a
PC BUS
50b
201
VIDEO CONNECTION UNIT
213
TDMS ENCODING UNIT
215
212
ENCRYPTION UNIT
214
AUTHENTICATION KEY EXCHANGE UNIT
HDCP ENCRYPTION UNIT
211
MULTIPLEX UNIT
DECODED VIDEO INFORMATION (RGB)
DECODED AUDIO INFORMATION

FIG.4

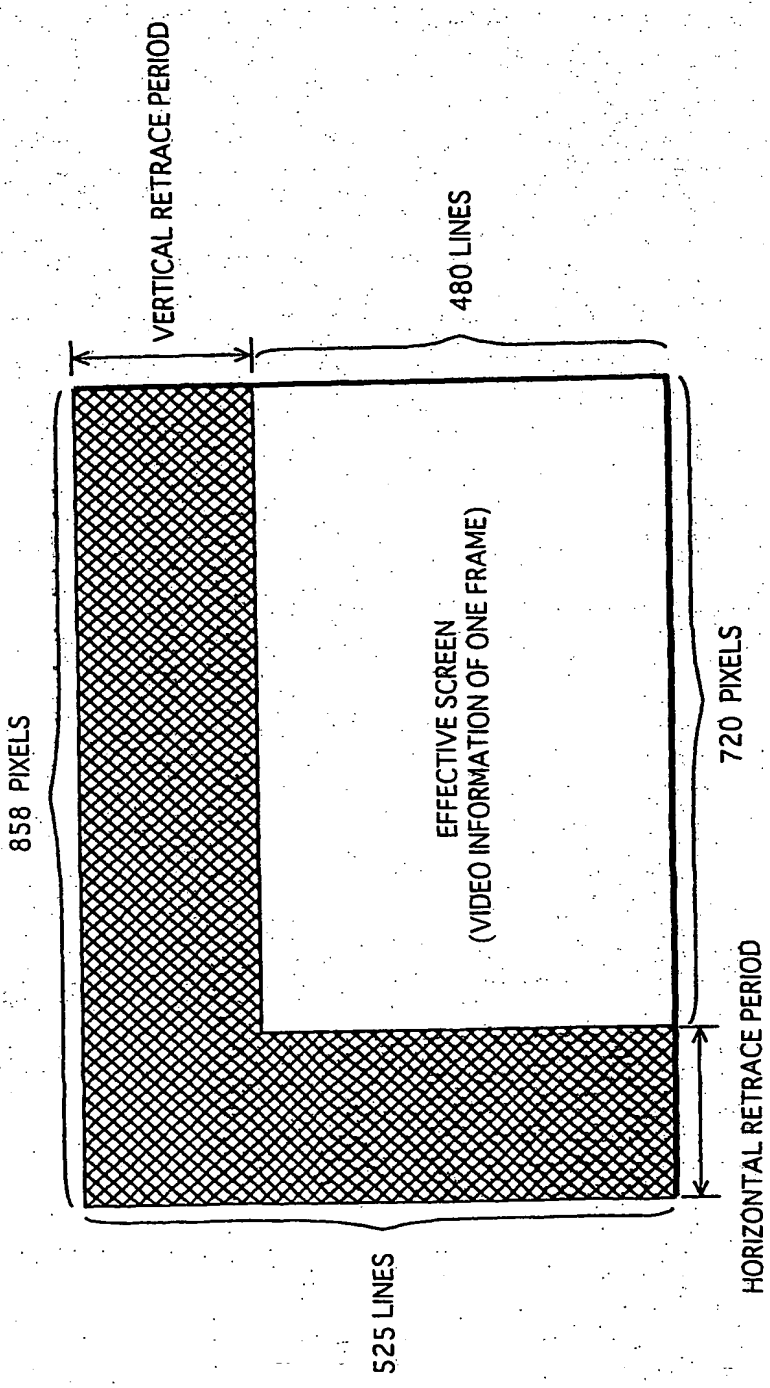

VERTICAL RETRACE PERIOD
480 LINES
858 PIXELS
EFFECTIVE SCREEN
(VIDEO INFORMATION OF ONE FRAME)
720 PIXELS
HORIZONTAL RETRACE PERIOD
525 LINES

FIG.5

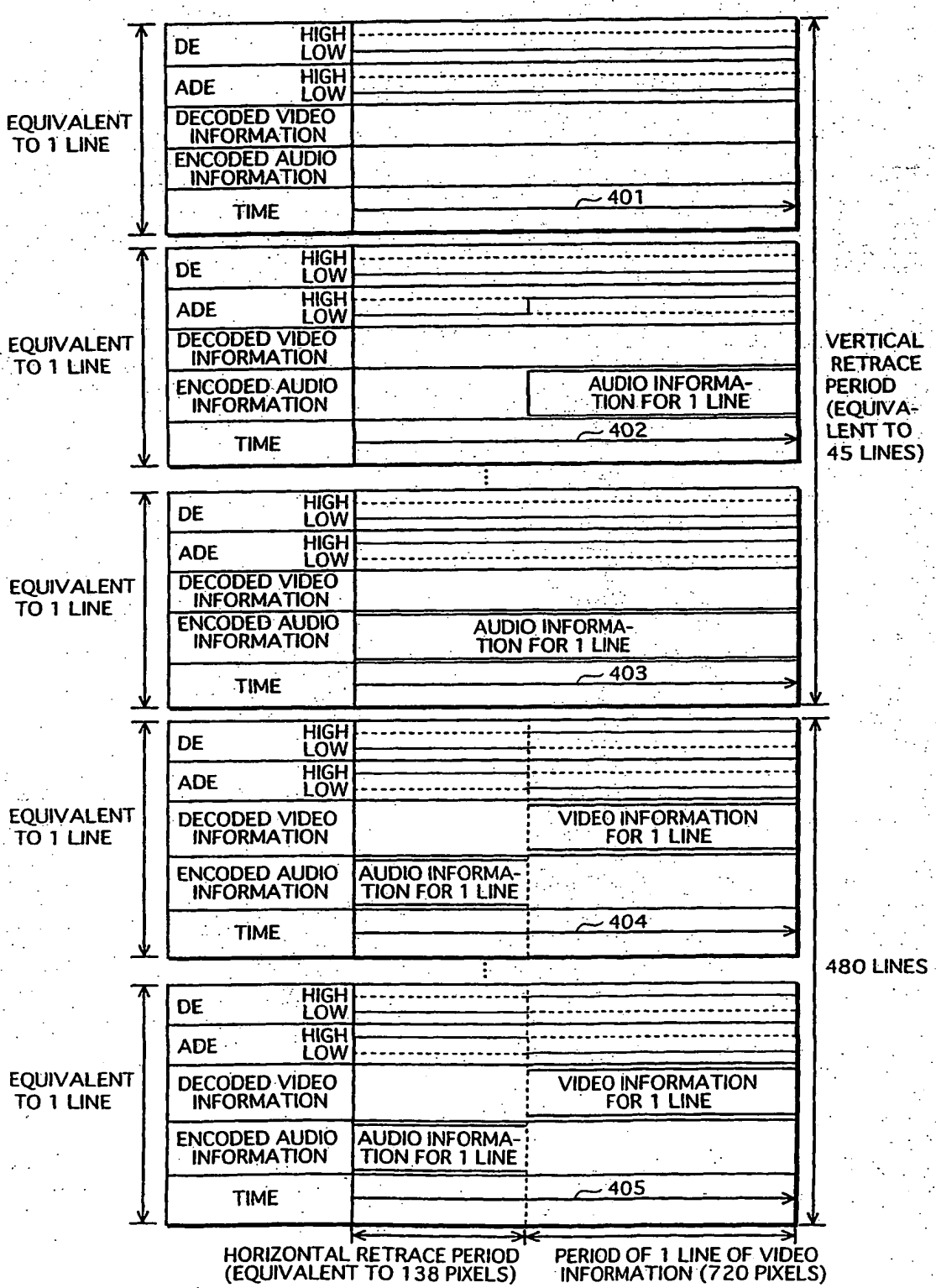

EQUIVALENT TO 1 LINE
DE
HIGH
LOW
ADE
HIGH
LOW
DECODED VIDEO INFORMATION
ENCODED AUDIO INFORMATION
TIME
401
AUDIO INFORMATION FOR 1 LINE
402
403
VIDEO INFORMATION FOR 1 LINE
404
405
VERTICAL RETRACE PERIOD (EQUIVALENT TO 45 LINES)
480 LINES
HORIZONTAL RETRACE PERIOD (EQUIVALENT TO 138 PIXELS)
PERIOD OF 1 LINE OF VIDEO INFORMATION (720 PIXELS)

FIG.6

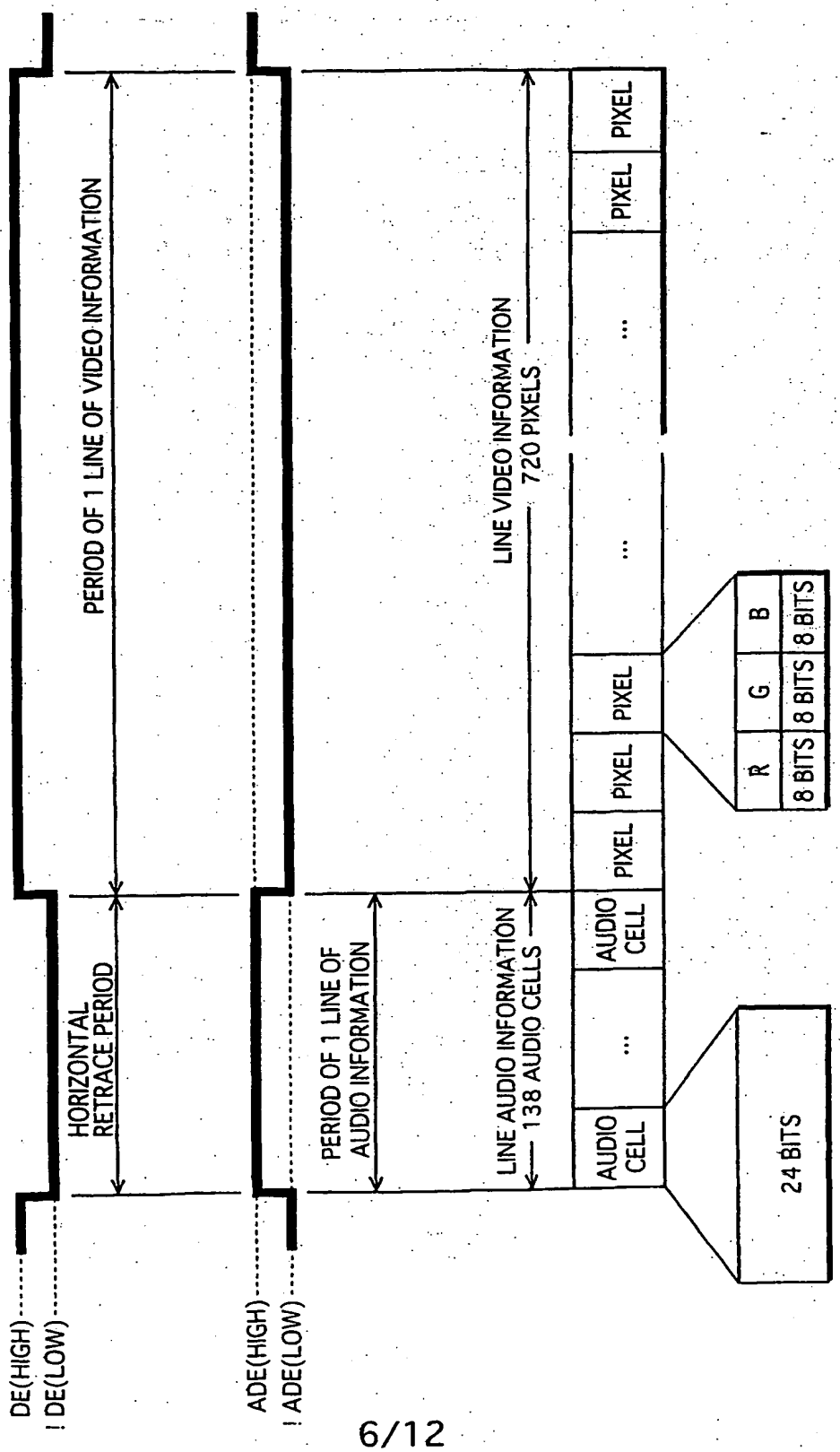

DE(HIGH)
! DE(LOW)
HORIZONTAL RETRACE PERIOD
PERIOD OF 1 LINE OF VIDEO INFORMATION
ADE(HIGH)
! ADE(LOW)
PERIOD OF 1 LINE OF AUDIO INFORMATION
LINE AUDIO INFORMATION 138 AUDIO CELLS
LINE VIDEO INFORMATION 720 PIXELS
AUDIO CELL
...
AUDIO CELL
PIXEL
PIXEL
PIXEL
...
PIXEL
PIXEL
24 BITS
R
G
B
8 BITS
8 BITS
8 BITS

FIG.7

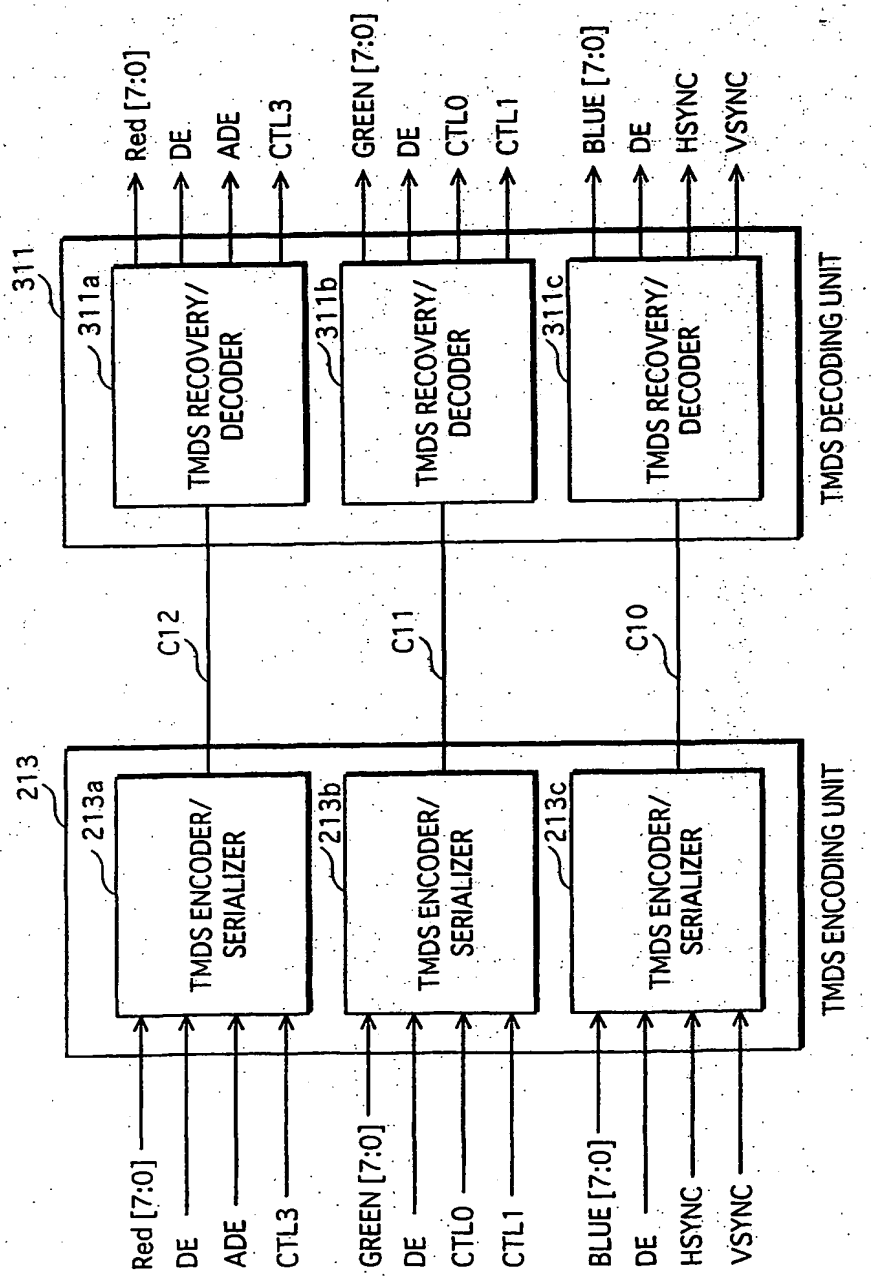

311
311a
TMDS RECOVERY/ DECODER
311b
TMDS RECOVERY/ DECODER
311c
TMDS RECOVERY/ DECODER
TMDS DECODING UNIT
Red [7:0]
DE
ADE
CTL3
GREEN [7:0]
DE
CTL0
CTL1
BLUE [7:0]
DE
HSYNC
VSYNC
C12
C11
C10
213
213a
TMDS ENCODER/ SERIALIZER
213b
TMDS ENCODER/ SERIALIZER
213c
TMDS ENCODER/ SERIALIZER
TMDS ENCODING UNIT
Red [7:0]
DE
ADE
CTL3
GREEN [7:0]
DE
CTL0
CTL1
BLUE [7:0]
DE
HSYNC
VSYNC

FIG.8

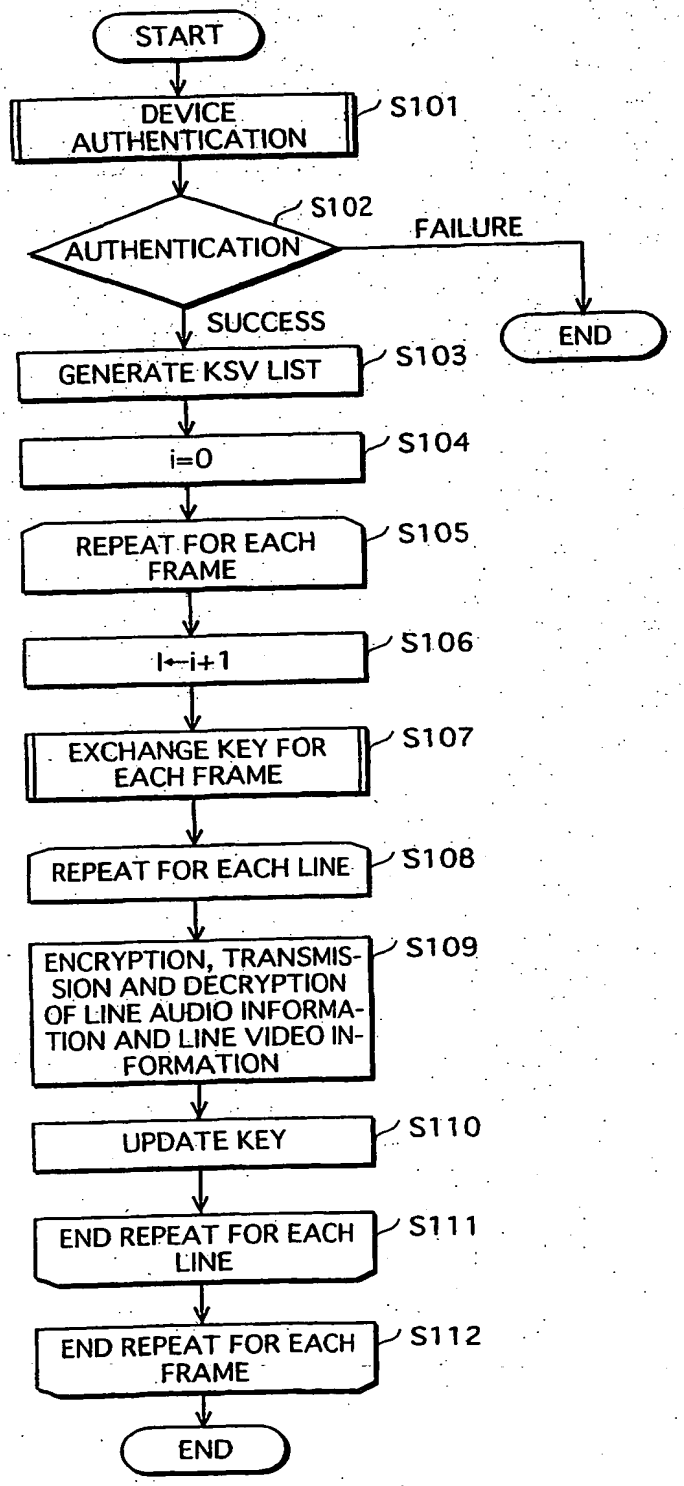

START
DEVICE AUTHENTICATION
S101
AUTHENTICATION
S102
FAILURE
END
SUCCESS
GENERATE KSV LIST
S103
i=0
S104
REPEAT FOR EACH FRAME
S105
I←i+1
S106
EXCHANGE KEY FOR EACH FRAME
S107
REPEAT FOR EACH LINE
S108
ENCRYPTION, TRANSMISSION AND DECRYPTION OF LINE AUDIO INFORMATION AND LINE VIDEO INFORMATION
S109
UPDATE KEY
S110
END REPEAT FOR EACH LINE
S111
END REPEAT FOR EACH FRAME
S112
END

FIG.9

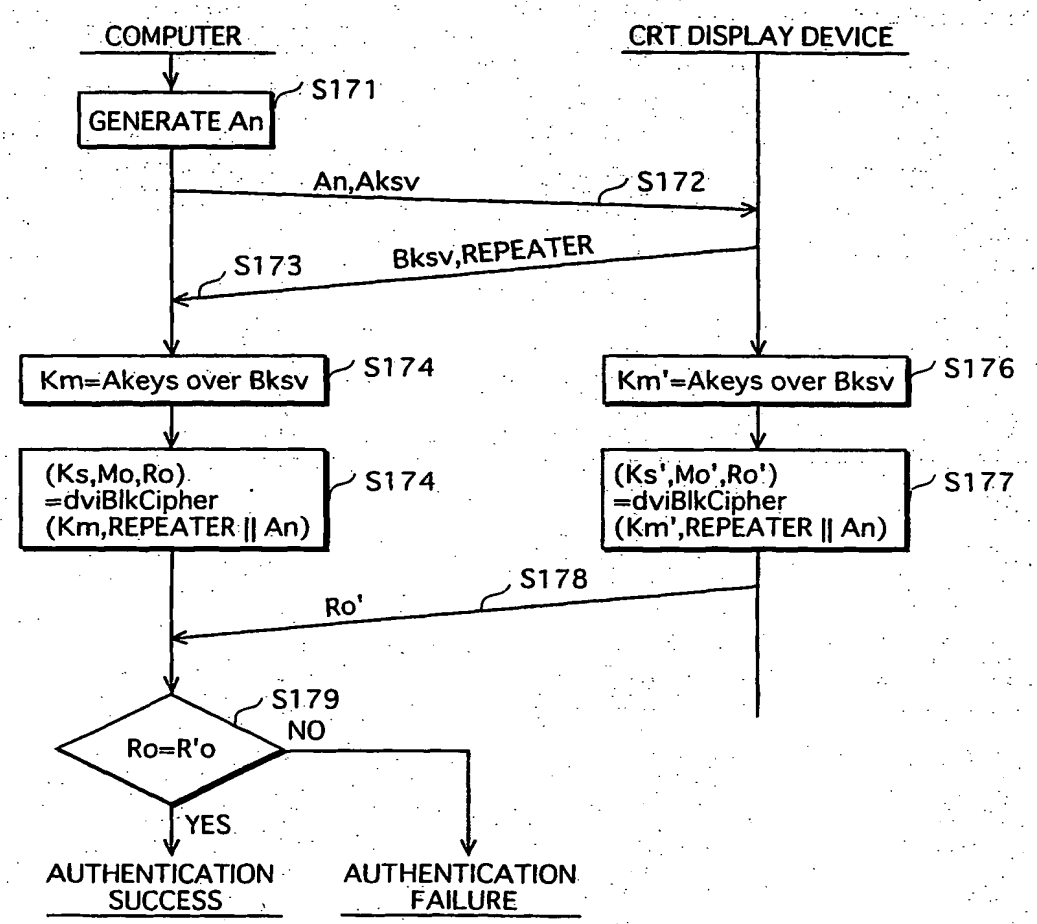

COMPUTER
CRT DISPLAY DEVICE
GENERATE An
S171
An,Aksv
S172
S173
Bksv,REPEATER
Km=Akeys over Bksv
S174
Km'=Akeys over Bksv
S176
(Ks,Mo,Ro)
=dviBlkCipher
(Km,REPEATER || An)
S174
(Ks',Mo',Ro')
=dviBlkCipher
(Km',REPEATER || An)
S177
S178
Ro'
S179
Ro=R'o
NO
YES
AUTHENTICATION SUCCESS
AUTHENTICATION FAILURE

FIG.10

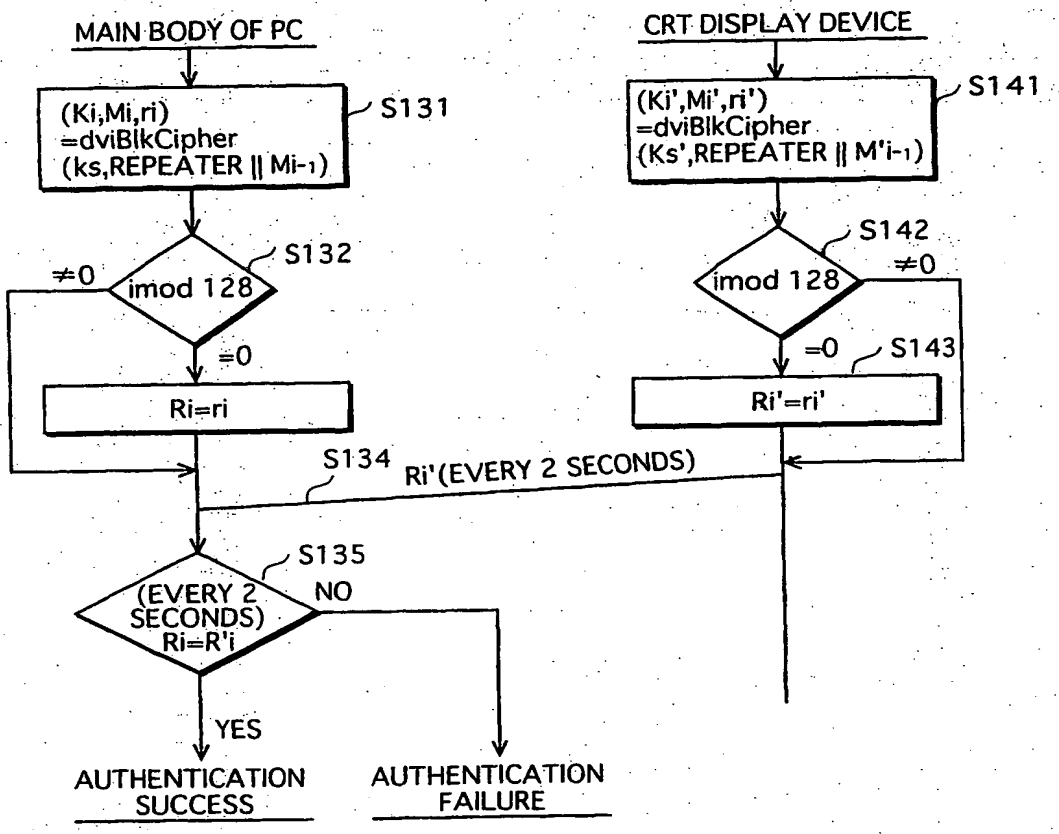

MAIN BODY OF PC
(Ki,Mi,ri)
=dviBlkCipher
(ks,REPEATER || Mi-1)
S131
imod 128
S132
≠0
=0
Ri=ri
CRT DISPLAY DEVICE
(Ki',Mi',ri')
=dviBlkCipher
(Ks',REPEATER || M'i-1)
S141
imod 128
S142
≠0
=0
S143
Ri'=ri'
S134
Ri'(EVERY 2 SECONDS)
(EVERY 2 SECONDS)
Ri=R'i
S135
NO
YES
AUTHENTICATION SUCCESS
AUTHENTICATION FAILURE

FIG. 11

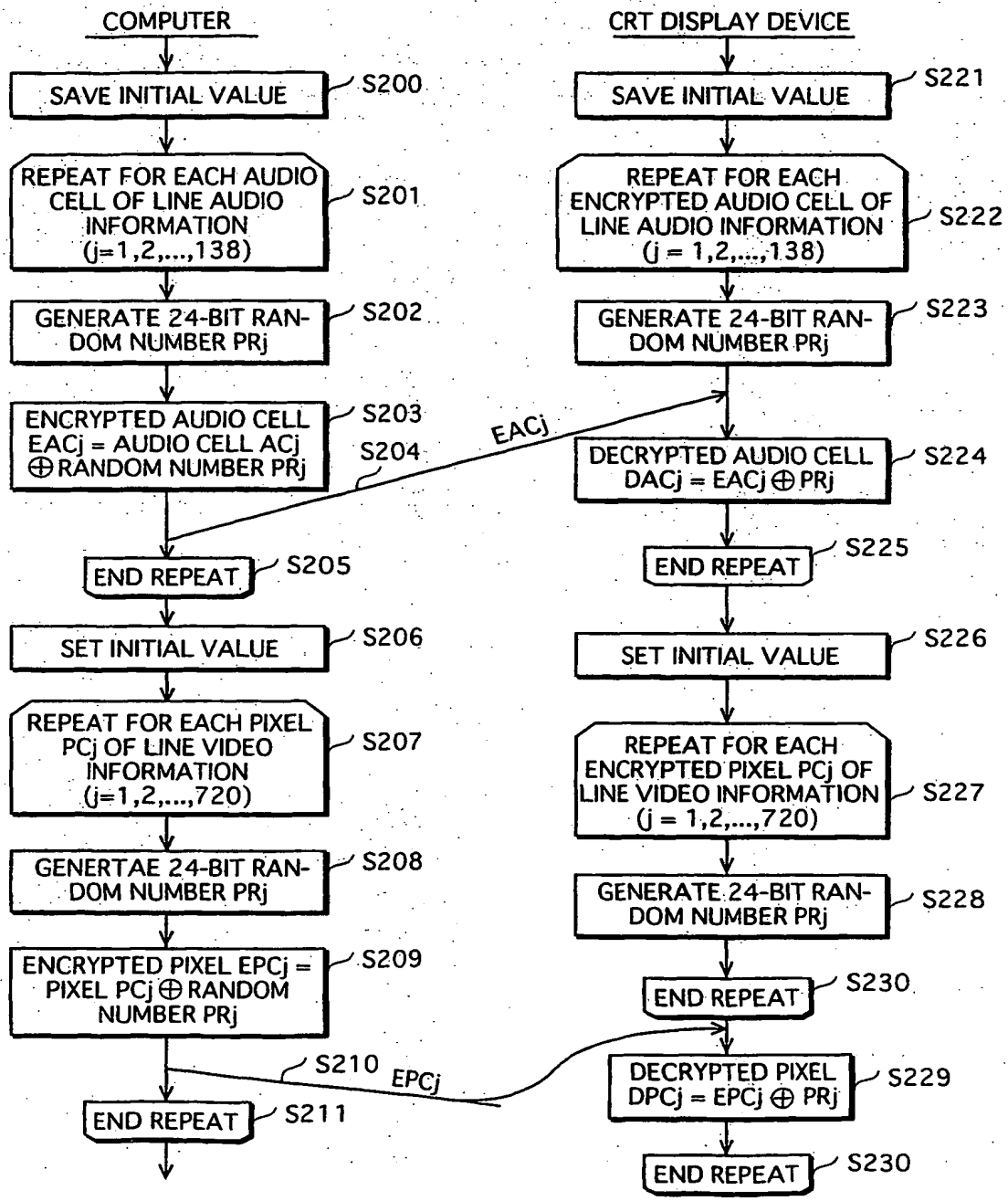
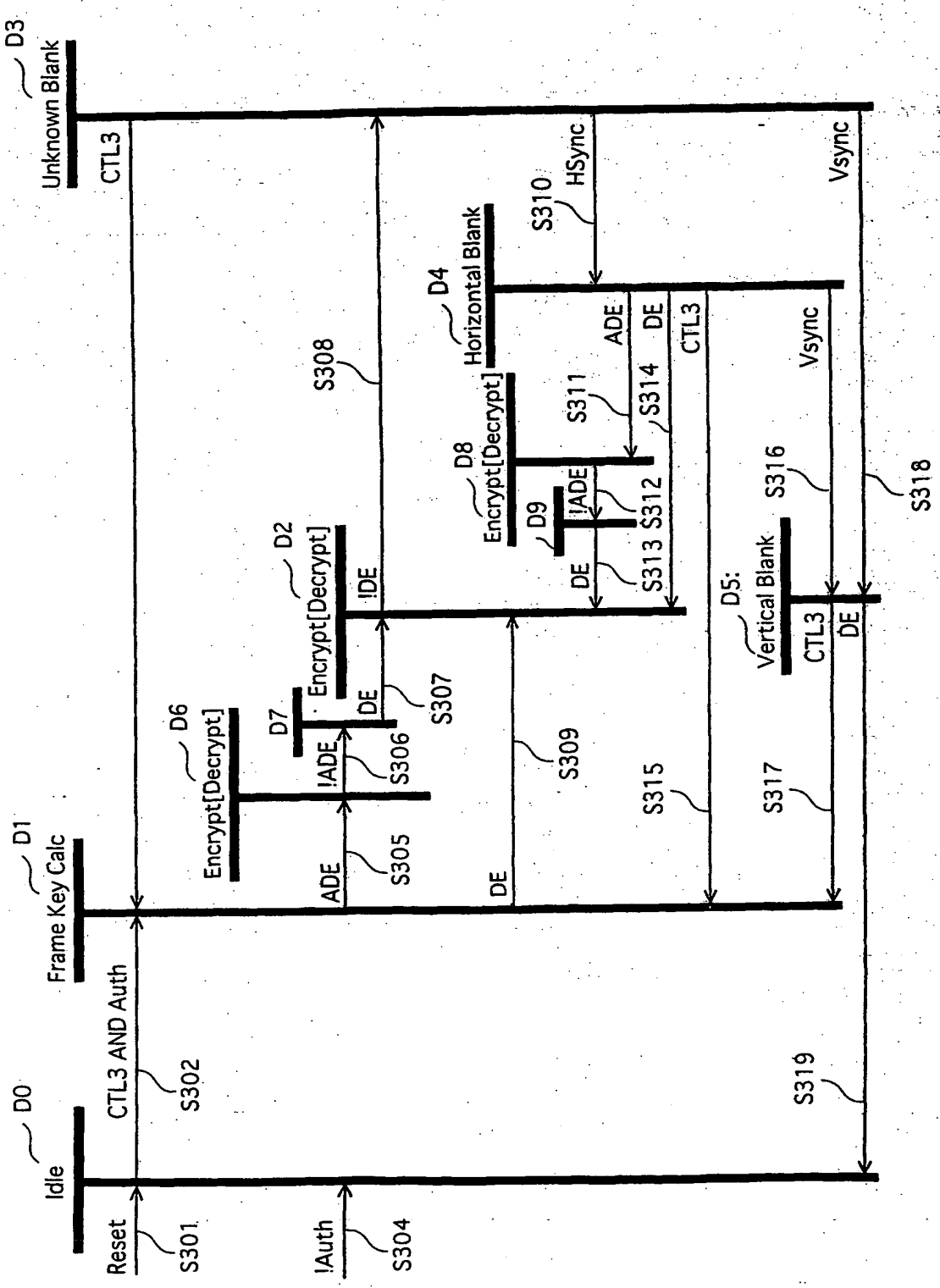

COMPUTER
SAVE INITIAL VALUE
S200
REPEAT FOR EACH AUDIO CELL OF LINE AUDIO INFORMATION (j=1,2,...,138)
S201
GENERATE 24-BIT RANDOM NUMBER PRj
S202
ENCRYPTED AUDIO CELL EACj = AUDIO CELL ACj ⊕ RANDOM NUMBER PRj
S203
S204
EACj
END REPEAT
S205
SET INITIAL VALUE
S206
REPEAT FOR EACH PIXEL PCj OF LINE VIDEO INFORMATION (j=1,2,...,720)
S207
GENERTAE 24-BIT RANDOM NUMBER PRj
S208
ENCRYPTED PIXEL EPCj = PIXEL PCj ⊕ RANDOM NUMBER PRj
S209
S210
EPCj
END REPEAT
S211
CRT DISPLAY DEVICE
SAVE INITIAL VALUE
S221
REPEAT FOR EACH ENCRYPTED AUDIO CELL OF LINE AUDIO INFORMATION (j = 1,2,...,138)
S222
GENERATE 24-BIT RANDOM NUMBER PRj
S223
DECRYPTED AUDIO CELL DACj = EACj ⊕ PRj
S224
END REPEAT
S225
SET INITIAL VALUE
S226
REPEAT FOR EACH ENCRYPTED PIXEL PCj OF LINE VIDEO INFORMATION (j = 1,2,...,720)
S227
GENERATE 24-BIT RANDOM NUMBER PRj
S228
END REPEAT
S230
DECRYPTED PIXEL DPCj = EPCj ⊕ PRj
S229
END REPEAT
S230

FIG.12


D0
Idle
D1
Frame Key Calc
D2
Encrypt[Decrypt]
D3
Unknown Blank
D4
Horizontal Blank
D5:
Vertical Blank
D6
Encrypt[Decrypt]
D7
Encrypt[Decrypt]
D8
Encrypt[Decrypt]
D9
Reset
S301
CTL3 AND Auth
S302
!Auth
S304
ADE
S305
!ADE
S306
DE
S307
!DE
CTL3
S308
DE
S309
HSync
S310
S311
ADE
S312
!ADE
S313
DE
S314
DE
CTL3
S315
Vsync
S316
S317
CTL3
DE
Vsync
S318
S319

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 June 2002 (27.06.2002)

PCT

(10) International Publication Number
WO 02/051150 A3

(51) International Patent Classification[7]: H04N 7/167

(21) International Application Number: PCT/JP01/11104

(22) International Filing Date:
18 December 2001 (18.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2000-383345 18 December 2000 (18.12.2000) JP

(71) Applicant *(for all designated States except US)*: **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.** [JP/JP]; 1006, Oazakadoma, Kadoma-shi, Osaka 571-8501 (JP).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MATSUZAKI, Natsume** [JP/JP]; 1-6-7-803, Aomadaninishi, Minou-shi, Osaka 562-0023 (JP). **TATEBAYASHI, Makoto** [JP/JP]; 1-16-21, Mefu, Takarazuka-shi, Hyogo 665-0852 (JP). **NISHIO, Toshiro** [JP/JP]; 89-11, Higashifunabashi 1-chome, Hirakata-shi, Osaka 573-1115 (JP). **SUZUKI, Hidekazu** [JP/JP]; 469-1, Tsutsui-cho, Yamatokooriyama-shi, Nara 639-1123 (JP).

(74) Agent: **NAKAJIMA, Shiro**; 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 531-0072 (JP).

(81) Designated States *(national)*: CN, US.

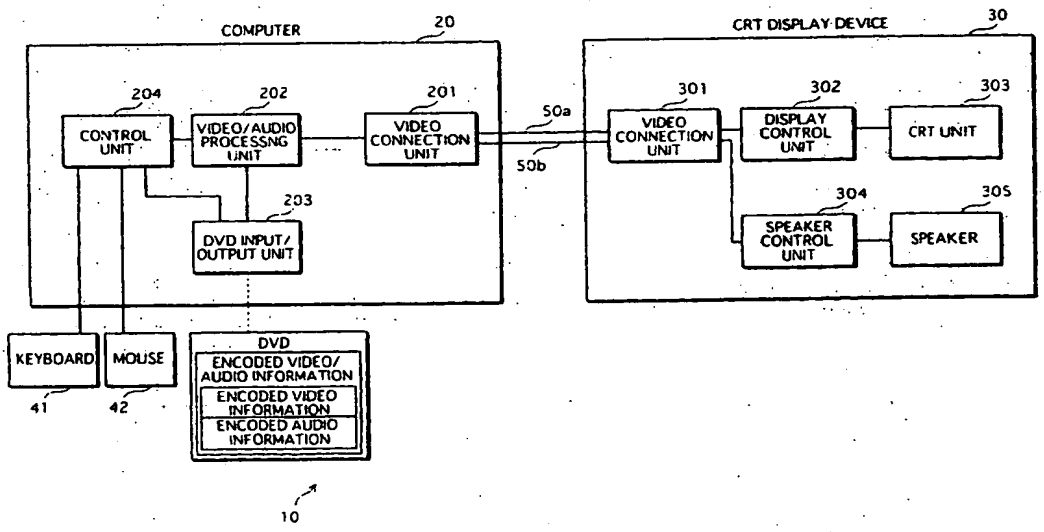
(84) Designated States *(regional)*: European patent (DE, FR, GB).

Published:
— *with international search report*

(88) Date of publication of the international search report:
9 January 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ENCRYPTION TRANSMISSION SYSTEM



(57) Abstract: A video signal and an audio signal are time division multiplexed, encrypted, and transmitted. A transmission side time-compresses the audio signal, multiplexes, encrypts, and transmits the time-compressed audio signal in a blanking period of the video signal. Control is performed using an audio signal data enable signal ADE, and a audio signal/video signal switch signal.

WO 02/051150 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/JP 01/11104

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 14626 A (SILICON IMAGE INC) 16 March 2000 (2000-03-16)	1
Y	page 1 -page 5 page 14, line 10 - line 16 figure 5	2,3,14
P,Y	EP 1 130 917 A (SONY CORP) 5 September 2001 (2001-09-05) column 1, line 30 - line 37 column 1, line 56 -column 2, line 4 column 3, line 16 - line 21 column 5, line 52 -column 6, line 1 figures 1,8	2,3,14

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 August 2002	30/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tito Martins, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/JP 01/11104

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MCCONNAUGHEY M: "A DIGITAL-INTERFACE STANDARD FOR DISPLAYS THE DVI INITIATIVE IS ALREADY CHANGING CRTS FOR THE BETTER AND IS DESTINED TO PROMOTE THE GROWTH OF FLAT-PANEL MONITORS" INFORMATION DISPLAY, PALISADES INSTITUTE FOR RESEARCH SERVICES, NEW YORK, NY, US, vol. 16, no. 1, January 2000 (2000-01), pages 18-21, XP000879888 ISSN: 0362-0972 the whole document ---	1-23
A	"DIGITAL VISUAL INTERFACE DVI" PAPER DIGITAL DISPLAY WORKING GROUP, XX, XX, 2 April 1999 (1999-04-02), pages 1-76, XP002948299 the whole document -----	1-23

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/JP 01/11104

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0014626 A	16-03-2000	AU 6034099 A	27-03-2000
		WO 0014626 A1	16-03-2000
EP 1130917 A	05-09-2001	JP 2001245270 A	07-09-2001
		CN 1311582 A	05-09-2001
		EP 1130917 A2	05-09-2001
		US 2001037307 A1	01-11-2001

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.